Exploring the Propagation of Fake Cyber News: An Experimental Approach

Michele Maasberg
La Tech University
maasberg@latech.edu

Emanuel Ayaburi
University of Texas at RGV
emmanuel.ayaburi@utrgv.edu

Charles Z. Liu
University of Texas at SA
charles.liu@utsa.edu

Yoris A. Au
Georgia Southern University
yau@georgiasouthern.edu

Abstract

The rising trend of fake news in cyberspace has escalated with increasing velocity of information exchange and an explosion of information sources. Combating fake news in the cyber security context is important due to its use as a content-based social engineering attack, or weaponization of information to compromise corporate information assets. This research aims to explore the proliferation of this type of threat through initial empirical analysis of propagation of cyber news with particular emphasis on potential for generation of weaponized information in the form of fake cyber news. Antecedents of the propagation of cyber news were examined using the Theory of Engagement. An exploratory experiment was conducted with 84 subjects in the field of cyber security on a social network platform. An analysis of the data showed that aesthetics and readability were important factors at the point of entry, but after initial engagement with the news, only novelty influenced propagation.

1. Introduction

On May 3, 2017, an anonymous user posted files on a discussion forum revealing that French presidential candidate Emmanuel Macron maintained an undisclosed shell corporation in the Caribbean [1], [2]. Although researchers determined that the files were fake, the news spread widely online up until France's presidential election on May 7, 2017 [2]. In addition, following a hack of 9GB of emails allegedly by Russian-backed group Fancy Bear, Macron's team had to release a public statement to clarify that not all of the information posted was genuine [3]. This has rendered cyber news, which is the propagation of news in cyber space, an important subject.

Fake news in the cyber security context, or *fake cyber news*, can be considered a content-based social engineering attack that may be difficult to detect [4]. Fake news has been implemented in a number of different contexts, including propaganda, elections, stock market manipulations, malware attacks, and advertising [4]. The affected parties are often forced to officially respond and comment on sensitive issues that should not have been discussed. Such responses often cause damage to the financial interests or reputation of the party involved, or ruin deals between organizations [5]. For example, firms have used fake news to attempt to influence stock prices for years, as in the case of ABM Capital influencing the stocks of FitBit by falsely claiming that it had approached FitBit's board about taking over the company [6].

To some, it is likely that fake cyber news has not been on the radar of IT security professionals as it has been considered "just another malicious payload delivered by an ecosystem that's already developed all sorts of tradecraft for doing just that" [5, para. 5]. However, the proliferation of fake cyber news is becoming a critical cybersecurity risk to address as it is used to seduce users into becoming victims of phishing, malware, and denial of service (DoS) attacks [5], [7]. The damage to corporate information assets by fake cyber news can have a broad impact if it gets out of hand due to ease of propagation concerns [7].

Propagation concerns from a cyber security standpoint are demonstrated on social media sites that can facilitate the spread of viewership quickly [7]. As such, a number of technology companies, including but not limited to Google, Facebook, and Twitter, have faced public scrutiny for the propagation of fake news [4]. During the recent U.S. presidential campaign, an analysis of engagement on Facebook showed that top fake news stories generated more engagement than top real news stories from 19 major news outlets (fake news generated 8,711,000 shares, reactions and comments while real news generated 7,367,000 of the same) [8]. Therefore, understanding the process of engagement with fake news in cyberspace appears to be a key element in inhibiting its propagation.

The purpose of this research is to understand how different the phenomenon of fake cyber news is and to determine the process and antecedents of its propagation. Specifically, we seek to address the following research questions.

RQ1: What factors influence the propagation of cyber news?

RQ2: Are participation and engagement different in the context of cyber news propagation (i.e., passive (reacting) as opposed to active (written feedback)?

URI: http://hdl.handle.net/10125/50357
ISBN: 978-0-9981331-1-9

RQ3: What informational characteristics aid in the propagation of cyber news?

To answer these questions, we examine prior literature to differentiate different categories of fake news, conceptualize fake cyber news, and develop a model of cyber news propagation using the Theory of Engagement.

2. Categorizing News and Fake Cyber News

Individuals read news for a variety of reasons. These could be due to curiosity, fear, a sense of urgency, polarization or a desire to stay up to date with world, national or local events, [9]. In recent years, the definition of news has been revisited in a number of different ways with the rise of computer mediated communication (CMC) [10]. Holders of the traditional view of news seek to define and understand news primarily from the formal journalism standpoint involving skills and activities for production of news by disciplined practitioners shrouded in tradition. The emerging "a *la carte*" model of news gathering defines the concept of news more by a broad spectrum of digital sources to include text, email, social networking sites, and blogs where the concept of news is defined more by the message, regardless of whether or not the source is verifiable [11], [12].

Customarily, the term "news" carries a sense of authority as the underlying assumption is that there exists an authenticity or legitimate standard to oversee and regulate news practices [12]. The normative dimension of journalism view contends that the phenomenon of news is a pursuit of knowledge through an epistemologically defensible standard of content creation that meets the standards of reliability, truthfulness, and independence manifested by proper gatekeeping, factuality and objectivity [12]. However, the advent of the Internet and the explosive growth of online media outlets make such traditional views obsolete and significantly expand the boundary of news propagation. In light of the penetration of fake news in cyber space, it is imperative to come up with a formal structure to distinguish fake news from real news or other categories of news, and examine the presumably different mechanisms of dissemination. Table 1 displays a general differentiation of real news from fake news based on the standards of *gatekeeping*, *factuality* and *objectivity* proposed in [12]. The concept of gatekeeping suggests that news production must involve the process of limiting its initiators to ensure the existence of quality control that weeds out trivial issues and prevents the sensationalizing of news. Factuality in the production of news implies the establishment of mechanisms to ensure a consumer can confirm its content based on evidence. Lastly, the initiator of news must not be influenced by strong emotion and remain rational and impartial. Elimination of emotion in the production of news ensures that the news is dispassionate. In the absence of the criteria of gatekeeping, factuality, and objectivity, fake news may arise.

Table 1. Real and fake news comparison [12]

Dimension	Real News	Fake News
Gatekeeping	Quality control; important over trivial; avoid sensational	Manipulation; editing or failure to edit
Factuality	Fidelity to evidence that can be checked by others; original reporting	Same set of facts interpreted differently or alternative facts
Objectivity	Dispassionate, unbiased, rational	Not autonomous from source or other entity

Communication and psychology literature have examined the fake news phenomenon over the last decade, but have viewed the phenomenon in the light of political satire [11], [13], [14]. The use of fake news as political satire does not necessarily have a negative connotation. Satire has been used for entertainment, information expansion, and promotion of public debate, often holding entities in positions of political power accountable for their behavior [11].

Current fake news terminology carries a negative connotation of intentionally fabricated articles aiming to manipulate reader's perception [15]. The surge in this type of fake news can be explained by 1) fewer barriers to entry in media industry 2) rise in social media platforms 3) decline of trust and confidence in mainstream media and 4) rise in political polarization [11]. Empirical studies have shown that high exposure to fake news and low exposure to real news have the effect of making consumers perceive fake news as real [13]. This results in the manipulation of readers' perceptions to achieve the initiators' varied motives. This suggests the need to categorize news based on motive as terminology evolves. Table 2 displays the different categories of news propagated and their underlying motivations.

Table 2. Categorization of news - motive [12]–[18]

Domain	Definition	Motive
Real news	Authentic content; standards of gatekeeping, factuality, and objectivity	Pursuit of knowledge through a discipline of verification
Fake news	Fictitious stories generated; disinformation	Push an agenda; deception
Satire	Unlikely to be misconstrued as factual	Entertainment
Bias	Objectivity failure in reporting, subject	Financial gain to sell news

	selection, or priority	
Conspiracy theories	Difficult to verify as true or false	Shock
Rumor	Unverified claims	Cope with anxiety and uncertainty
State sponsored propaganda	Government sanctioned sources in repressive states	Control
Unintentional reporting mistakes	Incorrect reports	No motive
False statements by politicians	Deliberately fabricated content by political figure	Ego; push a political agenda;
Supermarket tabloids	Partially true and outright false articles about well-known individuals	Entertainment

In addition to the various motivations summarized in Table 2, a newer, darker pattern of motivation has also emerged in the cyber security domain, begetting discussion as a subcategory referred to as *fake cyber news*, which is viewed as a content-based social engineering attack where the content becomes a weapon for compromising information systems [4], [7], [9]. For example, cyber attacks resulting from the fake news regarding Emmanuel Macron data should be differentiated from other unreliable news categories in Table 2. This is due to the nature of the attack vector (i.e., phishing domain), use of malware resulting data breach and subsequent disruption [3]. Table 3 displays a summary of arguments on the conceptualization of fake cyber news (as a specific subcategory of fake news) from the extant literature. As a subcategory, behavior of fake cyber news can be seen as similar to activities attributed to motivations of certain types of malware, for example *disruption* [19].

Table 3. Fake cyber news categorization arguments

Argument	**Discussion**	**Conclusion**	**Proposed Security Control**
Fake cyber news has an under-reported role in phishing scams [5]	Trained to be alert to phishing; too good to be true, warning role	Raises interesting issue of awareness and training	Administrative-preventive (i.e., security awareness training)
Fake cyber news is weaponization of information by nation states and cyber mercenaries [7], [9]	Attackers customize malware in fake news	Tailored lures propagated by victims in social circles enable large influence	Technical-preventive; technical-detective (i.e., monitoring tools)
False content online can affect organization and should be on IT professional's radar [5]	Security/IT are only teams in organizations that have the expertise; controlling the flow of fake information outside the company is a formidable task	Security must extend to protective monitoring to include external activity in fake news campaigns	Administrative-detective; Technical-detective (i.e., application level programmatic tools [5])
Fake cyber news propagates well on social media [4]	Using social media leads to self-imposed mental disconnect from cyber-hygiene	Social media users are likely going to propagate news they disagree with (i.e., policy issue for employee social media use)	Administrative-preventive; administrative-deterrent (i.e., issue specific security policy)
Fake cyber new works in different situations [5]	Event that causes fear is the perfect breeding ground for fake stories	Competition for attention is keen as stories appear as legitimate makes people believe them	Administrative-preventive; (Management supervising and monitoring, i.e., Management level brief or email)

As presented in Table 3, fake cyber news clearly violates the standards of *gatekeeping*, *factuality* and *objectivity*, and creates a formidable cyber security risk to be addressed by IT security personnel through administrative and technical security controls. *Fake cyber news is thus conceptualized as news propagated in cyber space with the intent of compromising information systems assets through the manipulation of its consumers.* We propose that cyber adversaries use fake cyber news as seduction in content based social engineering campaigns and continue to increase their level of sophistication along with complex payloads [7]. Frequency and severity of impact of fake cyber news becomes a point of risk assessment for organizations, making study of propagation a pertinent issue. Next, we examine a model of fake cyber news derived from the Theory of Engagement, where the nature of propagation is examined based on characteristics during the various stages of the propagation. The examination of propagation of cyber news with particular emphasis on potential for generation in the form of weaponized information, or

fake cyber news, sets the groundwork for understanding proliferation of weaponized fake news.

2.1. Conceptualizing Propagation of Cyber News - Theory of Engagement

Engagement can be defined as a positive, fulfilling work-related state of mind characterized by vigor, dedication, and absorption [20]. Engagement in the context of IT systems includes behavioral (observable actions) as well as cognitive and affective components. This means that it is defined not only by the state of interacting directly with a system but also by the emotional involvement of users [21]. The first known use of the concept of engagement in academic literature appears in Kahn's [22] description of how individuals in an organizational context "use varying degrees of themselves physically, cognitively, and emotionally in work role performances" [22, p. 692].

Kahn's [22] grounded theory approach led to the proposal of engagement as a multi-dimensional construct consisting of three dimensions (physical, cognitive and emotional) that an individual experiences simultaneously [23]. The three categories of engagement are not necessarily mutually exclusive. Engagement is considered an active state associated with high levels of cognitive activity and effort. The cognitive dimension of engagement has been an essential component in prior studies and concerns the association between the engaged state and high levels of cognitive activity directed towards performing the work role, which directly influence the emotional and physical reactions during the engagement process.

In the context of news digestion, engagement occurs when a cyber news consumer is immersed cognitively through the active verification of news, or emotionally through the show of likes of the news items. Subsequently, the physical expression of engagement occurs through a passive indication of interest or an active involvement in the spread of the information. Engagement is both a state and set of behaviors through three different stages—point of engagement, period of engagement, and disengagement/ reengagement—which can be operationalized as behavioral output [24]. As behavior could change through different states, we model the phenomenon of engagement in the propagation of cyber news as a process, and not an event, as shown in Figure 1.

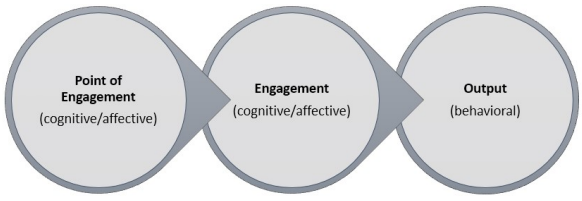

Figure 1. Proposed model of engagement (adapted from [24])

The process of engagement contains various constructs unique to the point of engagement, process of engagement, and the behavioral output. The following sections describe their nature and relationships.

2.2. Readability

Readability is a cognitive attribute of engagement at the point of engagement where the engagement process is initiated when the informational composition of the system interface catches a user's attention [24]. Readability refers to a measure of whether or not text matches the given reading skill level and background of the reader [25]. The concept of readability has often been studied in the context of educational materials where it is important to match the material construction to the target audience [25].

The persuasiveness of a cyber news article largely depends on its ability to motivate a reader to explore its content, which in turn depends on whether the reader can understand the substance of the article correctly. Hence, the ease of comprehension of the information contained in cyber news is important for improving the cognitive fit between content of the news and the reader's perception. When the news is very easy to read, the readers are more likely to be cognitively involved, resulting in a higher persuasiveness of the article. IT security professionals are a skeptical bunch [5], and therefore might not fall victims to fake cyber news as often. However, an unsophisticated reader might fall victim to social engineering or phishing attack that uses cyber news. It is therefore important to understand cyber news readability in the possible propagation of fake cyber news.

2.3. Source Credibility

Source credibility is another cognitive construct in the engagement process that may affect whether or not a user will continue engagement after obtaining the participants' initial interest and attention [24].

The intent of distributing news is to disseminate information. The news needs to be crafted and communicated in a manner that is convincing to its readers after they have been attracted by the title. The ability of a news article to maintain the attention of a consumer depends on the source credibility, which defines the competence, trustworthiness, and dynamism of the message source [26]. These three qualities of the source of the cyber news are valued characteristics that influence the perception of readers as they engage the news items. Readers having a high degree of competency and trustworthiness perception of news items were found to be more likely to find the news articles appealing and will spend more time on the news than they would with other news items.

In this study, we believe that perception of readability should impact perception of credibility of the source for users based on the Theory of Engagement. The idea is that if the text matches the reading skill and background of the user and the user becomes engaged, the user should stay engaged if based on that they form the perception that the source is trustworthy, competent and dynamic (credible). We hypothesize:

Hypothesis 1: Readability positively influences source credibility.

2.4. Aesthetics

Aesthetics is an affective attribute of engagement at the point of engagement where images, layout, and format of the news articles first catch the attention of users [24]. These characteristics of the appearance of cyber news articles can affect the judgment of readers as they process the information and decide on what actions to take. The aesthetics of the news items may affect the emotional processing of its information content and provoke some reaction from the reader. The level and kind of emotional responses depend on the extent of the reader's set of beliefs regarding the news. Thus, the degree of aesthetics in the news becomes the point of engagement with the news items. The higher the aesthetics the more likely readers will be attracted to the news items and begin the process of engagement. The effect of the aesthetics of news items could have a reinforcing effect on the extant beliefs about the news items' uniqueness and ability to foster further and deeper processing by readers. We argue that the aesthetics of news items serves as the point of rumination which eventually leads to a sustainable commitment with the news over a period of time.

2.5. Novelty

Various definitions of novelty have been proposed in previous research involving a comparative analysis of past and present experiences [27]. Since novelty is considered the antithesis of familiarity, it can be broadly defined as a change from routine that attracts attention. Novelty can also be considered a function of level of arousal, introducing the dimension of surprise as well as the psychophysiological nature of the construct [27]. Novelty in this study is defined as the degree to which readers view cyber news items as uncommon and unique in order to capture attention and facilitate deeper processing [27].

If a stimulus is novel, then the likelihood that users will engage in more elaborate information processing increases [28]. In marketing research, it has been shown that the likelihood of product purchase increased in the presence of novel discount presentation because consumers processed the discount information more accurately [28]. Firms are thus encouraged to design price-related presentations that consumers will view as uncommon or unique (novel) in order to capture the attention of consumers and motivate deeper processing, improving the rate of product purchase [28].

From an economic perspective, the novelty of the news plays a large role in its propagation as readers are overloaded with information. Novelty is pertinent viewing fake news from an economic viewpoint, as it can be considered a demand side problem since the users' determination to click on sexy headlines that lead them to sites of nefarious or unknown reputation perpetuate the fake news [18]. Thus, human nature in many cases to succumb to the desires of the senses creates a demand side problem that no social media algorithm tweak to deter fake news can address [18].

Based on the Theory of Engagement, aesthetics is considered a dimension at the point of entry, and novelty is consequently at the engagement period, where a user is theorized to be attracted by attention getting interfaces and then engagement maintained by a more elaborate information processing mechanism of novelty. Thus, we hypothesize:

Hypothesis 2: Aesthetics positively influences novelty.

2.6. Propagation (Active and Passive)

Propagation in this study refers to the physical behavioral output of users and can be either active or passive. We consider both the active and passive outputs since engagement shares some attributes with "flow" [29] which is a more passive state. We suggest that novelty experiences with cyber news intrinsically interesting and pleasurable require focused attention and stimulate curiosity. The stimulation of curiosity could lead to a passive response such as the show of interest, dislike or attention [24].

Information interaction provides the connectivity for engagement. Cyber news may be aesthetically appealing with design elements that promote novelty by individuals. The concentration of individuals on cyber news contribute to an engaging experience. An engagement with news due to novelty and verifiability results in an expression of that interactivity. These interactions may go beyond just expressing flow (passive act) to taking a memorable action. Therefore, the characteristics of the outcome of the period of engagement have two dimensions: passive (flow experience) such as likes and views, and active (interactivity) such as posts and comments. As verifiability and the uniqueness of cyber news affect readers processing of its information content, we hypothesize the following:

Hypothesis 3a: Source credibility positively influences active propagation.

Hypothesis 3b: Source credibility positively influences passive propagation.

Hypothesis 4a: Novelty positively influences active propagation.

Hypothesis 4b: Novelty positively influences passive propagation.

Previous research has suggested that education, age, and total media consumption can be strongly associated with individual's belief in their ability to discern whether headlines were true or false [15]. Hence we included age and social influence as controls in the study. Education and media consumption were not considered due to the fact that the sample of the study consists of exclusively undergraduate students.

2.7. Research Model

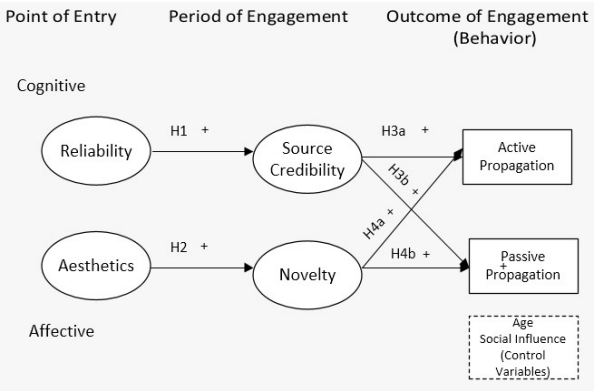

Figure 2. Proposed conceptual model

3. Methodology

3.1. Experimental Design and Subjects

Prior studies have suggested the measurement of actual behaviors, instead of intent, in an information security context [30]. To this end, we use an experimental approach to test the research hypotheses developed in Section 2. Subjects were recruited from cybersecurity classes from a large university in the Southwestern United States to participate in a class project hosted on a social media platform. Approximately 120 subjects were invited and 90 subjects agreed to participate. At the end of the study, a survey regarding their experience on the social network was administered to the participants and 84 of them provided valid responses, resulting in a response rate of 70%. At the beginning of the experiment, subjects received a detailed description of the task which required them to collect cyber security-related news and post them on a discussion forum created on the Slack social network platform. Figure 3 displays a sample of activity that took place on the platform. Some information propagated covered areas such as measures to protect electronic devices, pros and cons of some security initiatives and impact of some security incidents. At the end of the experiment, subjects were asked to take part in a survey which consisted of questions regarding subjects' perceptions of characteristics of cyber news and how it impacted their participation in the experiment. The survey specifically noted questions related to the propagation of cyber security news; and finally, demographic data was collected.

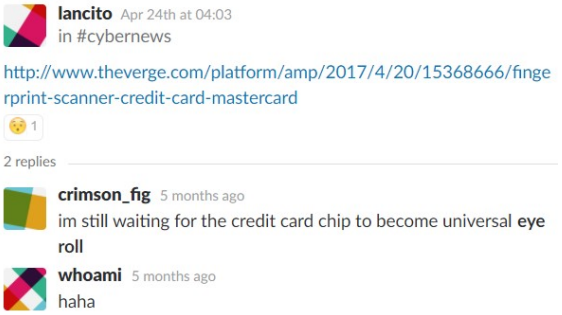

Figure 3. Sample of propagated cyber news

3.2 Operationalization of Variables

The research model includes six constructs. Each construct was measured with multiple items adapted from the extant literature to improve content validity [31]. Table 4 lists the operational definitions of the constructs.

Table 4. Variable operational definitions

Variable	Definition
Aesthetic (AU) [32]	Extent to which the cyber-news has a positive emotional effect on a subject eliciting response
Readability (RD) [33]	Level of comprehension of a cyber-news item by subjects
Source Credibility (SC) [34]	the extent to which the source of cyber-news is perceived to be believable, competent and trustworthy by subjects
Novelty (NV) [27]	The degree to which subjects view a cyber-news items as uncommon/unique in order to catch attention and facilitate deeper processing
Passive Propagation (PP)	Number of reactions (likes, emoticons, etc.)
Active Propagation (AP)	Number of written text responses.

3.3. Analysis Strategy

We tested the hypothesized relationships among the constructs using structural equation modeling (SEM) with SmartPLS v2.0 software. We chose a variance-based SEM implemented in SmartPLS v2.0 because we are studying a new phenomenon that requires the exploration of factors that are predictive of the propagation of fake cyber news. To avoid any misinterpretation of the relationship between constructs in the research model, we first verified the adequacy of

the measurement model before conducting a test of the hypotheses.

4. Results

Due to the setting of the experiment it is not surprising that 70% of the subjects were aged 20 to 30 years. However, there was a fair representation of younger and older age groups, making it possible to extend the interpretation of the results to other age groups. The focus of the study is on the sources and propagation of cyber security information. As such, the subjects were recruited from cyber security classes. The proportion of males is 67% which is consistent with the gender distribution in computer and information systems.

4.1 Measurement Model Validity

To validate the measurement model, construct validity was established through the examination of convergent and discriminant validity of the constructs, and reliability was established. Convergent validity was supported by large factor loadings for all constructs (shown in Appendix); all of the factor loadings showed good measure of the factor [35], [36].

The composite reliability scores for all the constructs are greater than the recommended minimum threshold of 0.7 (see the table in the Appendix). Therefore, the factor loadings and composite reliability provide support that the items measure the constructs for which they are hypothesized to measure, exhibiting adequate convergent validity and reliability.

Table 5. Correlations and AVE

Con.	AVE	AU	RD	SC	NV	PP	AP
AU	0.48	(0.69)					
RD	0.48	0.30	(0.69)				
SC	0.66	0.06	0.49	(0.81)			
NV	0.60	0.53	0.17	0.22	(0.77)		
PP	1.0	0.08	-0.01	0.26	0.20	(1)	
AP	1.0	0.05	0.13	0.01	0.28	0.49	(1)

Discriminant validity of each latent construct was tested using the method recommended by [37]. The square root of AVE of each construct should be higher than the correlation between the construct and any other constructs. This criterion is satisfied by all constructs (see the diagonal values in Table 5). Therefore, our measurement model exhibits sound reliability and validity necessary for the further testing of the research hypotheses.

Testing was conducted to assess the potential effects of common method variance (CMV) though Harman's single factor test [75]. All items were loaded on a single factor in an EFA with a single unrotated factor, the largest eigenvalue 8.722 explained 34.93% of variance, suggesting that the majority of variance is not accounted for by one general factor and therefore CMV is not a concern based on Harman's single factor test.

4.2 Structural Model Results

Estimates derived from the SEM structural analysis were used to test the research hypotheses. In the first two hypotheses, H1 & H2, we proposed relationships between points of engagement (readability and aesthetics) and period of engagement (source credibility and novelty) in cyber news propagation. The path coefficients for these relations as shown in Table 6 are positive and significant (H1 b=0.49, $p<$ 0.01; H2 b=0.583 $p<0.01$), suggesting that subjects who perceived the news items to be readable have higher tendencies of showing trust in the credibility of the news items. Also, high levels of perceived aesthetics of the news items lead subjects to high novelty views of the news items. Thus, our findings support H1 and H2. These results indicate that readability and aesthetics identified in the model development are potential points of interest in readers' engagement with cyber news.

Finally, a key argument in this research is that the novelty and source credibility of the cyber news items which are central during the period a subject engages the news items leading to the propagation of the news items. The propagation of the news items was hypothesized to either occur in an active fashion where subjects exert efforts to contribute to the thread of conversion of the news, or in a passive manner where they show interest in the news through signs of like or dislike. No significance (H3a, b=-0.05 $p>0.05$, H3b, b=-0.01, $p>0.05$) was found for the effect of source credibility on the propagation of the news in any form. However, the higher the novelty perception of the news items the subjects hold, the higher the likelihood of both the active and passive propagation of the news items (significant (H4a b=0.28, $p<$ 0.01; H4b b=0.19, $p<0.01$). For the control variables, only the social influence was found to be a significant predictor of cyber news propagation.

Table 6. Summary of results

Relationship Tested	Coef.	t-stat	Hypothesis	Result
RD → SC	0.49	7.260	H1	Supported
AS → NV	0.53	8.824	H2	Supported
SC → AP	-0.05	0.473	H3a	Unsupported
SC → PP	-0.01	0.135	H3b	Unsupported
NV → AP	0.28	3.238	H4a	Supported
NV → PP	0.19	2.043	H4b	Supported
Control				
SI → AP	0.32	2.5		Supported
SI → PP	0.25	1.622		Supported
AG → AP	0.13	1.019		Unsupported
AG → PP	0.03	0.324		Unsupported

5. Discussion

We drew on the Engagement Theory [20], [22], [24], [41], [42] to study why and how fake cyber security news is propagated. The Theory of Engagement presents a three-stage process—point of engagement, period of engagement, and output of engagement—as a model to understand the dynamic nature of cyber news transmission. The results of the study offer insights in various stages of the engagement process.

Point of Engagement - Individuals tend to approach action by liking the specific activity (i.e., engaging in cyber news) and choosing to forsake another activity online. This process requires subjects to show interest in the news items. We proposed that the act of showing interest was a dual process comprised of both cognitive and affective processes. To become engaged in the propagation of cyber news is not merely by observation, but also through direct experience. The cognitive process is through the mental processing of the information contained in the news item. The ability to process the news items depends on how clearly and easily the information contained can be gleaned with little effort. Since engagement is characterized by persistence [43], the results of our analysis indicate that the less the effort (i.e., better readability) required to process the information in the news items, the higher the likelihood of engaging with the news items through their positive perception (i.e., more source credibility).

Period of Engagement – The Theory of Engagement postulates that interest in activity culminates in its concentration and its enjoyment, and individuals self-select into an activity that is not routine. Non-routine activities that are stimulating lead to a longer involvement in those activities. Our results support this conjecture as the novelty of the news items was found to affect the likelihood of subjects engaging in the cyber news. Such engagement led them to actively propagate it through the provision or assimilation of messages related to the news items. Equally, subjects passively propagate cyber news if the news items are novel by either showing interest or likeness of the message.

On the other hand, the systematic processing of the news items to certify their veracity did not lead to enjoyment of the news. We argued that credible news would attract the attention of subjects, provide good information and persuade them to share or propagate the news. However, the results of the study suggested that no such relationship exists. This implies that although subjects cognitively analyze news items by reading and been able to certify the veracity, they are not intrigued enough to want to share or comment on such news.

The results of our experimental study suggested that within the interactive and dynamic process of cyber news dissemination, subjects' engagement represents a strategy essential for its propagation. The rationale underlying these assertions is that although engaged subjects play a key role through dual processing (cognitive and affective) of key indicators of information contained in the news items, the likelihood of actually propagating the news items is driven by the affective component of the news; by providing recommendations, thoughts or likes. This is consistent with the findings in the marketing literature that affective factors significantly affect individual experience of flow with an activity such as interacting with online materials [44].

Contribution – This study makes a number of theoretical contributions. First, the Theory of Engagement is extended into a new domain that focuses on understanding the mechanism for the propagation of cyber news. Prior studies of engagement exist predominantly in education and video games literature [24], [41]. We therefore contribute to the applicability of Engagement Theory to a broader information systems context in information retrieval and processing. By operationalizing propagation (active and passive) as the outcome of engagement, we extend the overall nomological network of the Theory of Engagement. Second, we adapted a longitudinal approach to understand the phenomenon of fake cyber-news propagation. Prior research has encouraged the use of longitudinal and experimental approaches to investigate behavioral issues related to information systems security. Our study helps to strengthen the explanatory power of theory on actual information systems security behaviors.

Practical Implications – From a practical standpoint, our research focuses on an important issue in need of attention if the goal of the computer-mediated communication (CMC) is to remain a trusted source of information dissemination. We investigated a dual process—cognitive and affective—of information dissemination. The findings suggest that the possibility of propagation of cyber news is strikingly dependent on how it attracts people and less on how intellectually enhancing it can be. This is significant for policy makers and communication gatekeepers who are trying to combat the spread of disinformation. From the perspective of the cyber news consumers, our research provides a guiding point for venturing into the deep sea of information sources to make a better judgement of the kind of news items to spend their precious time on.

6. Conclusion and Future Research

This study examined the propagation of cyber news in order to lay the foundation for understanding fake cyber news propagation. Based on the Theory of Engagement, a longitudinal experimental study was conducted on a social network with 84 subjects to understand the nature of their assimilation and propagation of news. Our results show that subjects initiated engagement by both cognitive and affective processing of readability and aesthetics. However, they only continued the engagement process to the output stage through the affective process of novelty and less dependent on the cognitive process of source credibility. The output included both passive and active aspects of cyber news propagation operationalized through reactions to news as well as text responses.

As with any study, limitations exist. We recognize the limitations of the inherent bias in self-reports. Another limitation is regarding propagation across platforms. Most importantly, we recognize the value of inclusion of fake cyber news in the empirical study. Future research on a larger scale will include insertion of fake cyber news by confederate actors to address such concerns.

This exploratory study is part of a more extensive research that aims at systematically analyzing the propagation of fake cyber news. The current study was designed to first understand the basic propagation of news in the cybersecurity context and will serve as a platform for the more granular research on the nature of the propagation of the fake cyber news. The research in the next stage will focus on examining strategies to lower type 1 and type 2 errors with fake news, which refer to erroneously interpreting legitimate news as fake news, or not being able to identify fake cyber news, respectively. Data collection on users' propagation and perceptions regarding known real and fake news will help us better understand the nature of the phenomenon and contribute to the body of literature and provide practical technical solutions for the reduction of the propagation of fake news, particularly cyber fake news. Understanding the nature of type 1 and type 2 errors are expected to enhance current detection methods such as improving the algorithms and programmatic tools used to detect suspicious fake cyber news [5].

References

[1] D. Gauthier-Villars, "U.S. Hacker Linked to Fake Macron Documents, Says Cybersecurity Firm," *The Wall Street Journal*, 16-May-2017. [Online]. Available: https://www.wsj.com/articles/u-s-hacker-linked-to-fake-macron-documents-says-cybersecurity-firm-1494929136. [Accessed: 18-May-2017].

[2] E. Geller, "Neo-Nazi Activist May Be Behind Fake Macron Documents," *Politico*, 17-May-2017. [Online]. Available: http://www.politico.eu/article/neo-nazi-activist-may-be-behind-fake-macron-documents/. [Accessed: 18-May-2017].

[3] M. Burgess, "The Emmanuel Macron Email Hack Warns Us Fake News is an Ever Evolving Beast," *Wired*, 08-May-2017. [Online]. Available: https://www.wired.co.uk/article/france-election-macron-email-hack. [Accessed: 18-May-2017].

[4] S. Logan, "Fake News as a Cybersecurity Risk Plus Other Security Headlines," *Scam of the Week: Fake News*, 08-Dec-2016. .

[5] J. Fruhlinger, "What Fake News Means for IT - and How IT Security Can Help Fight It," *CSO Resources/White Papers*. [Online]. Available: http://www.csoonline.com/article/3153358/security/what-fake-news-means-for-it-and-how-it-security-can-help-fight-it.html. [Accessed: 01-Feb-2017].

[6] R. Nieva, "Fitbit CEO Says There's No Mysterious Takeover Offer," 10-Nov-2016. [Online]. Available: https://www.cnet.com/news/fitbit-ceo-james-park-denies-reports-of-mysterious-takeover-abm-capital/. [Accessed: 26-May-2017].

[7] B. Botezatu, "Beware of Fake News - From a Cybersecurity Standpoint," 02-Feb-2017. [Online]. Available: https://businessinsights.bitdefender.com/fake-news-cybersecurity. [Accessed: 15-Jun-2017].

[8] C. Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook," 16-Nov-2016. [Online]. Available: https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.fo83lzgJx#.euj5Daw0P. [Accessed: 26-May-2017].

[9] M. Kassner, "Extra, Extra! That Fake News Story Might Come With Malware," 19-Jan-2017. [Online]. Available: http://www.techrepublic.com/article/extra-extra-that-fake-news-story-might-come-with-malware/. [Accessed: 21-Jan-2017].

[10] A. Abbasi and H. Chen, "CyberGate: A Design Framework and System for Text Analysis of Computer-Mediated Communication," *MIS Quarterly*, pp. 811–837, 2008.

[11] R. Marchi, "With Facebook, Blogs, and Fake News, Teens Reject Journalistic 'Objectivity,'" *Journal of Communication Inquiry*, vol. 36, no. 3, pp. 246–262, 2012.

[12] S. L. Borden and C. Tew, "The Role of Journalist and the Performance of Journalism: Ethical Lessons From 'Fake' News (Seriously)," *Journal of Mass Media Ethics*, vol. 22, no. 4, pp. 300–314, Oct. 2007.

[13] M. Balmas, "When Fake News Becomes Real: Combined Exposure to Multiple News Sources and Political Attitudes of Inefficacy, Alienation, and Cynicism," *Communication Research*, vol. 41, no. 3, pp. 430–454, 2014.

[14] R. L. Holbert, "A Typology for the Study of Entertainment and Politics," *American Behavioral Scientist*, vol. 49, no. 3, pp. 436–453, 2005.

[15] H. Allcott and M. Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives*, vol. 31, no. 2, pp. 211–236, May 2017.

[16] R. L. Rosnow and E. K. Foster, "Science Briefs: Rumor and Gossip Research," Apr-2005. [Online]. Available: http://www.apa.org/science/about/psa/2005/04/gossip.aspx. [Accessed: 30-May-2017].

[17] The Self Agency, LLC, "B.S. Detector," 2017. [Online]. Available: http://www.apa.org/science/about/psa/2005/04/gossip.aspx.

[18] J. Shafer, "The Cure for Fake News is Worse Than the Disease," 22-Nov-2016. [Online]. Available: http://www.politico.com/magazine/story/2016/11/the-cure-for-fake-news-is-worse-than-the-disease-214477. [Accessed: 30-May-2017].

[19] A. R. A. Grégio, V. M. Afonso, D. S. F. Filho, P. L. de Geus, and M. Jino, "Toward a Taxonomy of Malware Behaviors," *The Computer Journal*, vol. 58, no. 10, pp. 2758–2777, Oct. 2015.

[20] D. Ford, S. E. Myrden, and T. D. Jones, "Understanding 'Disengagement from Knowledge Sharing': Engagement Theory Versus Adaptive Cost Theory," *Journal of Knowledge Management*, vol. 19, no. 3, pp. 476–496, May 2015.

[21] H. L. O'Brien, "The Influence of Hedonic and Utilitarian Motivations on User Engagement: The Case of Online Shopping Experiences," *Interacting with Computers*, vol. 22, pp. 344–352, 2010.
[22] W. A. Khan, "Psychological Conditions of Personal Engagement and Disengagement at Work," *The Academy of Management Journal*, vol. 33, no. 4, pp. 692–724, Dec. 1990.
[23] E. Soane, C. Truss, K. Alfes, A. Shantz, C. Rees, and M. Gatenby, "Development and application of a new measure of employee engagement: the ISA Engagement Scale," *Human Resource Development International*, vol. 15, no. 5, pp. 529–547, Nov. 2012.
[24] H. L. O'Brien and E. G. Toms, "What is User Engagement? A Conceptual Framework for Defining User Engagement with Technology," *Journal of the American Society for Information Science and Technology*, vol. 59, no. 6, pp. 938–955, Apr. 2008.
[25] S. Badarudeen and S. Sabharwal, "Assessing Readability of Patient Education Materials: Current Role in Orthopaedics," *Clinical Orthopaedics and Related Research®*, vol. 468, no. 10, pp. 2572–2580, Oct. 2010.
[26] A. C. Johnston and M. Warkentin, "The Influence of Perceived Source Credibility on End User Attitudes and Intentions to Comply with Recommended IT Actions," *Journal of Organizational End User Computing*, vol. 22, no. 3, pp. 1–21, Sep. 2010.
[27] T.-H. Lee and J. Crompton, "Measuring Novelty Seeking in Tourism," *Annals of Tourism Research*, vol. 19, no. 4, pp. 732–751, 1992.
[28] H. M. Kim and T. Kramer, "'Pay 80%' Versus 'Get 20% Off': The Effect of Novel Discount Presentation on Consumers' Deal Perceptions," *Marketing Letters*, vol. 17, no. 4, pp. 311–321, Dec. 2006.
[29] M. Csikszentmihalyi, *Flow. The Psychology of Optimal Experience*. New York (HarperPerennial), 1990.
[30] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future Directions for Behavioral Information Security Research," *Computers & Security*, vol. 32, pp. 90–101, Feb. 2013.
[31] D. Straub, M.-C. Boudreau, and D. Gefen, "Validation Guidelines for IS Positivist Research," *Communications of the Association for Information Systems*, vol. 13, no. 1, p. 63, 2004.
[32] H. H. Chang and S. W. Chen, "Consumer Perception of Interfact Quality, Security, and Loyalty in Electronic Commerce," *Information & Management*, vol. 46, pp. 411–417, 2009.
[33] T. Kanungo and D. Orr, "Predicting the Readability of Short Web Summaries.pdf," presented at the WSDM '09, Barcelona, Spain, 2009.
[34] A. Bhattacherjee and C. Sanford, "Influence Processes for Information Technology Acceptance: An Elaboration Likelihood Model," *MIS Quarterly*, vol. 30, no. 4, pp. 805–825, 2006.
[35] K. Zhu and K. L. Kraemer, "Post-Adoption Variations in Usage and Value of E-Business by Organizations: Cross-Country Evidence from the Retail Industry," *Information Systems Research*, vol. 16, no. 1, pp. 61–84, Mar. 2005.
[36] B. G. Tabachnick and L. S. Fidell, *Using Multivariate Statistics*, 5th ed. Boston: Pearson/Allyn & Bacon, 2007.
[37] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, vol. 18, no. 1, p. 39, Feb. 1981.
[38] N. K. Malhotra, S. S. Kim, and A. Patil, "Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," *Management Science*, vol. 52, no. 12, pp. 1865–1883, 2006.
[39] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common Method Biases in Behavioral Research: a Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology*, vol. 88, no. 5, p. 879, 2003.
[40] P. M. Podsakoff, S. B. MacKenzie, and N. P. Podsakoff, "Sources of Method Bias in Social Science Research and Recommendations on How to Control It," *Annual Review of Psychology*, vol. 65, pp. 539–569, 2012.
[41] N. Whitton, "Game Engagement Theory and Adult Learning," *Simulation & Gaming*, vol. 42, no. 5, pp. 596–609, Oct. 2011.
[42] P. M. Di Gangi and M. Wasko, "Social Media Engagement Theory: Exploring the Influence of User Engagement on Social Media Usage," *Journal of Organizational and End User Computing*, vol. 28, no. 2, pp. 53–73, Apr. 2016.
[43] J. W. Marcum, "Out with Motivation, in with Engagement," *Global Business and Organizational Excellence*, vol. 19, no. 4, pp. 57–60, 2000.
[44] S. Cai and Y. Xu, "Designing Not Just for Pleasure: Effects of Web Site Aesthetics on Consumer Shopping Value," *International Journal of Electronic Commerce*, vol. 15, no. 4, pp. 159–188, Jul. 2011.

Appendix – CR, Factor Loadings, Items

Construct and Items	**Loading**
Aesthetics: CR=0.78	
AS1: I feel comfortable surfing cyber news at these websites	0.68
AS2: The cyber news sites allows me to interact with other social network members	0.73
AS3: I think that the cyber news site engaged me to investigate more cyber security information	
AS4: The cyber news site made me think that I am a unique cyber security professional user of the site.	0.80
Readability CR=0.78	0.52
RD1: The cyber news I read allowed me to quickly scan and understand its gist	
RD2: The cyber news I read had text clearly intended to be read by a human	0.68
RD3: The cyber news I read generally contained complete sentences, coherent excerpts of sentences, or understandable titles	0.85
RD4: The cyber news I read looked nice, without garbage characters, wingdings, all caps	0.70
Credibility: CR=0.89	0.86
SC1:The person/organization providing the cyber news was knowledgeable on this topic.	
SC2:The person/organization providing the cyber news was trustworthy.	0.82
SC3:The person/organization providing the cyber news was credible.	0.85
SC4:The person/organization providing the cyber news appeared to be an expert on this topic.	0.71
Novelty: CR=0.85	
NV1: I like to find myself on cyber news websites where I can explore news and different things.	0.87
NV2: I want to experience customs, and cultures different from those in my own environment online.	0.83
NV3: I enjoy the change of environment which allows me to experience something new online.	0.76
NV4: I want there to be a sense of discovery involved as part of my online cyber news experience.	0.61