Government Information Quarterly 34 (2017) 307–316

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Cyber-rumor sharing under a homeland security threat in the context of government Internet surveillance: The case of South-North Korea conflict

K. Hazel Kwon[a,*], H. Raghav Rao[b]

[a] Walter Cronkite School of Journalism and Mass Communication, (Mail Code: 3051), 555 N., Central Ave. Suite 302, Arizona State University, Phoenix, AZ 85004-1248, USA

[b] Department of ISCS, COB, University of Texas at San Antonio, San Antonio, TX 78249, USA

ARTICLE INFO

Keywords:
Cyber rumor
Government Internet surveillance
Homeland and National Security
Information policy
Governance over cyberspace
Citizen distrust

ABSTRACT

Cyber-rumors and falsehoods have increasingly become a hindrance to government strategic communication. Especially when there is a national security alert, anti-government rumors can become weapons that thwart government crisis information management. A key element for any government's successful cyber-rumor management is to understand what makes citizens prone to engaging in cyber-rumors. We focus on citizens' cyber-rumoring tendency that arises within the larger context of a nation's governance over the Internet. Specifically, this study examines how citizen's assessment of government Internet surveillance influences their engagement with cyber-rumors during a homeland security threat. Two surveys in South Korea find that citizens' government Internet surveillance concerns *increased* their cyber-rumor sharing intention, and the effect was particularly significant during the period of homeland security threat. This paper reconsiders the efficacy of government Internet surveillance in mitigating cyber-rumor propagation among general public, and expands the discussions by introducing the logic of 'distrust effect' on cyber-rumoring. Cyber-rumor monitoring through government Internet surveillance can be counterproductive to homeland security efforts unless government aligns its surveillance policy with citizens' informational norms on cyberspaces.

1. Introduction

Cyber-rumors, falsehoods, and fake news have increasingly become adversarial forces in the efficient functioning of government. Cases are found in various national contexts, for example the mass exodus of citizens due to hate cyber-rumors in Bangalore, India and the inability of government to manage the situation (Srivasta & Kurup, 2012) as well as the impact of recent fake news on Western democracies. Especially when national security is at risk, cyber-rumors can become deepen the rift between public and government (Bernardi, Cheong, Lundry, & Ruston, 2012).

Detection of malicious activities that bring risks to national security and public safety has been a primary motive for many governments—including South Korea, the regional focus of this study—to adopt domestic Internet surveillance practices as part of cyber-defense and national security programs (Landau, 2013). The goal of deterrence, for example against adversarial activities such as terrorists' social media accounts for propaganda, illicit hacking, or fake news websites, seems obvious. However, defining the boundary of such targets in the context of cyber-falsehood is much trickier because rumormongering essentially depends on the extent to which such rumors are accepted by *ordinary citizens*. Citizens who believe, endorse, and share such rumors with other peer citizens could become 'unintended conspirators' for cyber-rumor propagation. In this sense, to successfully mitigate cyber-rumoring, government should be able to not only detect adversaries in cyberspaces but also understand why and when citizens become willing to engage with cyber-rumors, as opposed to relying on government official sources as a means of verification.

The current study contends that citizens' cyber-rumor sharing tendency is partly influenced by their assessment of, and concerns about government Internet surveillance programs because Internet surveillance is inherently contestable with regards to citizens' informational privacy and free speech (de Bruijn & Janssen, 2017; Newell, 2014). Freedom House (2016) reports that a steady decline in global Internet freedom coincides with enhanced government surveillance over the cyberspace. One possibility is that the restricted informational privacy and free speech could result in so-called "Foucauldian" effect such that the domestic Internet surveillance produces censorship effect on the governed in terms of what is safe to communicate and what is not (Christie, 1972; Foucault, 1977; Lyon, 2015). Under Foucauldian

* Corresponding author.
E-mail addresses: khkwon@asu.edu (K. Hazel Kwon), he.rao@utsa.edu (H. Raghav Rao).

http://dx.doi.org/10.1016/j.giq.2017.04.002
Received 3 January 2017; Received in revised form 14 April 2017; Accepted 15 April 2017
Available online 25 April 2017
0740-624X/

logic, citizens may draw back from sharing sensitive rumors if they are concerned about the government's Internet surveillance and its punitive potential. Despite the compromise of civil rights to some degree (i.e., free speech and privacy), government Internet surveillance in this scenario may be nonetheless thought to fulfill its instrumental goals because it probably helps reduce the spread of falsehood among general publics. However, an alternate narrative is that citizens' concerns about the Internet surveillance do not decrease, or perhaps aggravate, their willingness for cyber-rumoring? The efficacy of government Internet surveillance at the cost of civil rights needs to be understood.

To our knowledge, this study is the first attempt to empirically examine the threat of Internet surveillance in mitigating cyber-rumor propagation among the general public. Specifically, we explored the relationship between citizens' Internet surveillance concerns and cyber-rumor sharing tendency in the context of South Korea. As of 2016, South Korea is categorized as being "partly free" on the Net (Freedom House, 2016), with several manifestations of the punitive power of Internet surveillance (Lyu, 2012). For example, the nation's Cyber Bureau operated by the National Police Agency was legitimized under the National Security Law, and has arrested several domestic users for cyber-rumoring cases (You, 2015). The current project was launched in South Korea's political context, and we initially anticipated that results that would be consistent with the Foucauldian logic (self-censoring effect on cyber-rumoring).

The study's findings, however, suggest the *opposite* patterns: In fact, citizens' concerns about government Internet surveillance *increased* their willingness to engage in cyber-rumor sharing, and this tendency was particularly strong when the homeland security was on alert. Accordingly, this paper is organized with an intent to explain this rather counterintuitive result. In discussing the results later, we introduce an alternative logic, which we refer to as a 'distrust proposition' of cyber-rumoring. The central position of this logic is that the government Internet surveillance concerns contribute to loss of citizens' overall faith in government's informational integrity (Nissenbaum, 2004, 2015; Reddick, Chatfield, & Jaramillo, 2015). Such loss may cause the citizens to then engage in the propagation of anti-government rumors more readily, and their tendency to rely on such rumors could become more heightened in a threatening situation where there is an urgency for informational needs (Lee, 2009).

The rest of paper is organized as follows. Section 2 contextualizes theoretical considerations to draw hypotheses and research questions pertinent to cyber-rumoring in South Korea. Section 3 describes the research designs based on the replicated surveys during a homeland security threat and non-threat situation. Section 4 shows the results. Section 5 discusses the key findings and introduces the logic of distrust hypothesis on cyber-rumoring by focusing on the relationship between citizens' government Internet surveillance concerns and their willingness for cyber-rumor sharing. Finally, the study discusses its limitations and the directions for future research.

2. Theoretical considerations

Rumors are "claims of fact – about people, groups, events, and institutions – that have not been shown to be true, but that move from one person to another, and hence have credibility not because direct evidence is known to support them, but because other people seem to believe them" (Sunstein, 2009, p. 6). Studies of wartime and terrorism show that a homeland security threat is opportune for rumormongering because citizens would consume any information regardless of factuality, as far as it reduces their sense of uncertainty and anxiety (Allport & Postman, 1965; Fine, 2005; Knapp, 1944; Rosnow, 1980; Shibutani,1966; Starbird, Maddock, Orand, Achterman, & Mason, 2014; Kwon, Bang, Egnoto, & Rao, 2016). The information quality is often less important for rumor circulation than the subjective belief and the level of anxiety provoked by the message and by the situation (DiFonzo & Bordia, 2007).

2.1. Cyber-rumoring and internet surveillance in South Korea

Rumoring is a "social" as well as psychological phenomenon, which "indirectly acknowledges the political contexts in which they arise" (Edy & Risley-Baird, 2016, p.589). In this paper, we consider cyber-rumoring is distinctive from interpersonal rumor transmissions in that it arises within a larger landscape of the nation's governance over cyberspace, (i.e., Internet surveillance).

In regards to cyber-rumoring, government's Internet surveillance is a double-edge sword. Outwardly, government Internet surveillance could prevent cyber-rumors from spiraling by cultivating institutional- or self-censorship culture (Deibert, 2003; Wang & Hong, 2010). A well-known example is China's Internet censorship that prevents citizens from collective information sharing and from organizing anti-government actions in cyberspaces (King, Pan, & Roberts, 2013). At the same time, however, since government Internet surveillance often requires "backdoor access" to data (de Brujin & Janssen, 2017, p.2), such surveillance practices could decrease citizens' overall faith in government as a transparent informational actor, and subsequently divert their attention onto unofficial informational sources, and even worse, reinforce their beliefs in anti-government rumors.

A troubling part from the government point of view is that cyber-rumors can become rapidly viral and transformed into more damaging narratives via memetic processes in social networks unless citizens are ready to accept official rumor refutation as fact-checking material (Kwon, Oh, Agrawal, & Rao, 2012; Shin, Jian, Driscoll, & Bar, 2016; Starbird et al., 2014). Indeed, a case study of South Korea during a military threat finds that majority of cyber-rumors spread among the social media publics contained derogatory propositions against its government, which revealed obvious deviations from official reports (Kwon et al., 2016). In other words, the more citizens accept cyber-rumors at the moment of national insecurity, the greater is the misunderstanding between government and civil society, which can weaken the effectiveness of government information management (Bernardi et al., 2012; Lee, 2009). In this sense, governments perceive rumors to "have a negative impact on strategic communication efforts" and "influence people in ways contrary to those in power" (Dalziel, 2013a, p.3).

To respond to such conflicting effects of cyber-rumoring on public minds, some countries—including South Korea—have used the Internet surveillance program as a means of rumor monitoring at the cost of civil rights (Dalziel, 2013b; Jaeger, Betot, & McClure, 2003; Pavone & Degli Esposti, 2010). In South Korea, government Internet surveillance has become noticeably aggressive since 2004 under the "real-name verification" policy which resulted in nontrivial arrests of anti-government users (Kwon & Cho, 2015; Leitner, 2009). South Korea's cyber-rumor surveillance was particularly unobtrusive in 2010 when North Korea launched a missile attack on South Korea territory: multiple domestic users were indicted for cyber-rumoring under the rhetoric of the National Security law (Lyu, 2012; You, 2015). Some cases of such arrestments received harsh criticisms, thought to be the government's invasion of citizen privacy (Lyu, 2012). Although the real-name verification law was annulled in 2012, government Internet surveillance policy has not shrunk at the time this study was conducted (Cho & Kwon, 2015).

However, the efficacy of South Korean government's Internet surveillance for its homeland security information management is vague due to the paradox of government Internet surveillance as described above (censoring falsehood at the cost of citizens' faith in government transparency). On the one hand, collective experience of free speech and privacy violations could make citizens shy away from engaging with anti-government rumors online. On the other hand, the violation of civil rights by the Internet surveillance can aggravate distrust in public's minds, which leads to a greater reliance on rumors contradictory to the government channel of information. Moreover, the threat situation could facilitate citizens' consumption of cyber-rumors

due to the urgency for informational needs. Considering that this study is the first attempt to address the effect of government Internet surveillance on citizens' cyber-rumor sharing, we posit the two research questions below:

RQ1. How do citizens' government Internet surveillance concerns influence their cyber-rumor sharing tendency?

RQ2. Is there a differential effect of the government Internet surveillance concerns on cyber-rumor sharing between a homeland threat situation and non-threat situation?

2.2. Social psychological approach to cyber-rumor sharing in national threat situation

Social psychology studies on rumor transmission help understand motivations underlying individual citizens' cyber-rumor sharing. Earlier studies have pointed out two primary factors of rumor sharing: belief and anxiety. First, citizens' belief in rumor story is not necessarily based on the message's factuality. Rather, it is subjected to a message recipient's cognitive predisposition, for example, one's social identity (Einwiller & Kamis, 2009), personal relevance to the consequence that the rumor story implies (Liberman & Chaiken, 1991), and trustworthiness of the message senders (Garrett, 2011; Oh, Agrawal, & Rao, 2013). Rumor belief becomes particularly important when there is a high level of anxiety invoked by the rumor story (Rosnow, Esposito, & Gibney, 1988). Likewise, the anxiety invoked by rumor message (a.k.a., message anxiety) has been known as one of the most important antecedents of rumor transmission (Pezzo & Beckstead, 2006). Although a recent content analysis of social media rumors in the context of terror events found the message anxiety effect (Oh et al., 2013), there has not yet been systematic research that examines the ways in which belief and anxiety induced from a rumor message influence citizens' cyber-rumor sharing intention. Accordingly, we build on the existing rumor studies to explore whether citizen's cyber-rumor sharing is influenced by their belief in rumor messages and the level of anxiety induced from the message.

H1a. Citizens' willingness for cyber-rumor sharing will be influenced by their belief in a rumor message.

H1b. Citizens' willingness for cyber-rumor sharing will be influenced by the level of anxiety induced from the message.

In addition to the message-level factors, a threat situation is a contextual force that facilitates rumor propagation (Pezzo & Beckstead, 2006). Especially, a homeland threat event invokes a sense of terror in public minds. Social psychology literature has suggested that individuals manage their feeling of terrors by engaging in various social behaviors, for example religious activities, and scapegoating of others (Solomon, Greenberg, & Pyszczynski, 1991). Rumormongering is one way to collectively manage fear associated with the threat situation (Li, Vishwanath, & Rao, 2014; Shibutani, 1966). Whereas the effect of situational anxiety has been unclear in experimental studies—for example, positive effect found in Walker and Beckerle (1987) as opposed to insignificant effects found in Rosnow, Esposito, and Gibney (1988) and Kimmel and Keefer (1991)—studies that investigate the threat situational effect in the real-world context are very rare. This study examines the threat situational effect on citizens' cyber-rumor sharing intention by comparing citizen responses between during a homeland security threat and a non-threat situation.

H2. Citizens's willingness for cyber-rumor sharing will be greater in a homeland security threat than in a non-threat situation.

3. Research design

This research has two goals: to examine (1) social psychological factors underlying South Korean citizens' cyber-rumor sharing and (2) the effect of South Korean citizens' government Internet surveillance concerns on their cyber-rumor sharing, in the context of a homeland security threat. Fig. 1 summarizes the proposed research model.

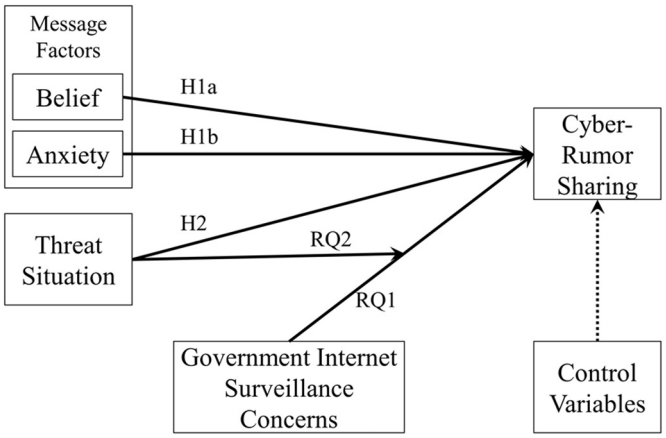

Fig. 1. Research design summary.

To address the difference between the national threat and non-threat situation, we systematically designed the two surveys. The first round of survey was in late February 2013 when a sense of crisis was heightened due to South-North saber rattling. Choosing this period was appropriate because our main interest was to understand cyber-rumor propagation during a homeland security threat. The second round of survey was conducted two years later, in August 2015, for comparing the results between the threat and non-threat situation. Given that the military tension between South and North Korea has been chronic, the second survey period was chosen after a period of South-North tension when an official apology was issued by North Korea, a rare event, and the threat level was momentarily lowered. We purposefully did not collect data in 2014 given an unusual national circumstance: the military conflict had become a secondary affair due to another nation-wide crisis event—Sewol Ferry disaster—that swamped the public minds throughout the whole year.

Conventionally, a replication study intends to confirm whether the original results are reproducible (Hubbard, Vetter, & Little, 1998). In the current study, the purpose is opposite: The survey was replicated to confirm whether the original results are specifically more prominent in the threat situation than in non-threat situation.

3.1. Survey 1

3.1.1. Survey context: South-North Korean saber rattling in 2013

In February and March 2013, South Korea's national security was alarmed by the provocation of North Korea that had launched its third nuclear weapon test (Jung & Park, 2014). A few saber-rattling incidents followed, including South Korea's announcement of their readiness to engage in warfare, UN Security Councils' sanction on North Korea, beginning of US-Korean military drills, and North Korea's attempt to annul the Korean Armistice that had lasted for 60 years. Uncertainty was particularly high because both Koreas had newly inaugurated leaders, whose foreign policies were not known to each other. Such leadership transitions contributed to increasing a sense of insecurity. A Gallup poll during that period (February 2013) reported that 76% of Korean citizens agreed that the incident posed a threat to peace in the Korean Peninsula, and more than half of the citizens perceived the situation to be “highly dangerous”. The tension between the two Koreas lasted for about two months.

3.1.2. Participants

A total of 311 South Korean online users were recruited based on a convenience sampling from a major survey company's nationwide panel

of 117,289 potential participants who used the survey company's mobile app[1]. The recruitment message was simultaneously sent out as a "study alert" either through the installed mobile app or via the survey company's homepage. The invitation message informed participants that this study aimed to understand citizens' opinions regarding the conflict with North Korea. The survey was automatically closed as soon as the expected sample size was attained in the following day. Respondents received the company's 'points' as a reward, which could be monetized if accumulated to some extent. While we could not assess the response rate due to the automated process, the recruitment was considered free from systematic biases given that the expected sample size was reached in less than two days. However, we note a possible bias due to the nature of voluntary participation, by which the topically interested could have participated in the survey more willingly than indifferent individuals. To enhance representativeness of different ages and genders, quota sampling was employed, which allocated about 60 respondents in each of five age groups (under 24, between 25 and 34, between 35 and 44, between 45 and 54, and older than 55) with roughly equal gender ratio. Based on the quotas, e-mail solicitations were sent out. Participants were instructed that the survey was confidential and their information would not be shared.

3.1.3. Real rumor-based scenario design

To gauge online users' rumor sharing intention, a scenario-based design was employed. Scenario-based design intends to measure user behavioral intentions in a realistic setting (Siponen & Vance, 2010), and is particularly useful when measuring sensitive responses in a nonintrusive way (D'Arcy, Hovav, & Galletta, 2009). Considering the potential sensitivity of rumor sharing under the homeland security threat situation, a scenario-based method was appropriate to our study. While most extant scenario-based research provides participants with a hypothetical setting (Siponen & Vance, 2010), we instead used real stories found from online platforms at the time of the incident. We chose three unverified cyber-rumors that were relevant to the military conflict, and shared in social media during the threat situation. We not only chose a story that was particularly widespread during the given period but also included two other stories, similar versions of which have been circulated periodically in the past. These two other stories were intentionally selected for the consideration of survey replication during a non-threat situation, to minimize a message novelty effect. Rumor stories were as follows:

(1) Iranian involvement in North Korea nuclear weapon test (*Rumor 1*): This rumor raised suspicions about whether the Iranian government had supported North Korea to advance nuclear weapons technology. A mutated version of the story included information about the physical presence of Iranian scientists at test sites in North Korea.
(2) Preemptive attack plan by the U.S.-South Korea joint forces (*Rumor 2*): This rumor about the joint forces' preemptive attack against North Korea's further nuclear pursuit had been recycled and re-circulated from the past incident of North Korea's nuclear test in 2009. Akin to the story about Iranian involvement, this story evoked fear by associating the incident with possibility of physical warfare.
(3) Sexual assault of a South Korean female by one of the US military soldiers (*Rumor 3*): This rumor was said to be under-reported due to the threat from North Korea. While not directly about the North Korean threat, the third story was reflective of negative sentiment toward the US-Korea military alliance among subcultural groups in South Korea, and similar narratives have been recurring historically.

These rumors were chosen based on fear-appeal, and the potential to produce miscommunication between citizen and government. More specifically, Rumor 1 was picked considering that it was one of the most widespread rumors and directly elicited fear from the national threat. Rumors 2 and 3 were chosen due to the anti-government connotations, conveying unwelcome messages to the publics: Rumor 2 implied possible launching of warfare, which is the last option the Korean public would support; and Rumor 3 not only directly discredited the government's pro-USA policy but also risked US-Korean relationships. Note that these stories were the real stories found in cyberspaces during the period. We selected them in order to be as realistic as possible. Also, we examined multiple rumor messages instead of a single message to examine whether results are consistent across different rumor characteristics.

3.1.4. Measurements

The dependent variables were rumor sharing willingness for each rumor. Independent variables were message-level factors (i.e., belief and anxiety), government internet surveillance concerns, and the homeland security threat situation (i.e., the survey period). The complete items for the measurement instruments are presented in Table 1. All variables were measured using a seven-point Likert type scale, unless specifically mentioned.

3.1.4.1. Dependent variable. To measure the dependent variable, *cyber-rumor sharing intention*, a single-item question asked respondents their willingness to share each rumor via online channels (they were asked to mark the highest score if they had ever shared the rumor). We tried to define 'online channels' as broadly as possible, asking this question by giving various examples including email, online chatting, discussion boards, and social media. Each rumor-related question was randomly rotated to prevent the ordering effect. Cyber-rumor sharing intention was asked by a single-item, instead of multiple-items, considering the current scenario-based design. In scenario-based design, measurement errors tend to be minimal because respondents are asked their behavioral intention unambiguously, "immediately following the scenario" (Siponen & Vance, 2010, p. 7). Besides, a single-item measure increases response rate, helps reduce missing values, and the use is recommended when evaluating unidimensional and unambiguous constructs (Bergkvist & Rossiter, 2007; Wanous, Reichers, & Hudy, 1997). Most rumor studies are indeed based on scenario designs with a single-item measure to ask respondents' rumor belief and sharing willingness (e.g. Einwiller & Kamins, 2009; DiFonzo & Bordia, 2007; Pezzo & Beckstead, 2006).

3.1.4.2. Independent variables. (1) Rumor message-related variables included *message belief* and *message anxiety*. For message belief, respondents were asked whether they believed each rumor message to be true (no belief = 0; belief = 1). Message anxiety was measured by two-item questions that asked how much respondents felt that the rumor message was anxiety-invoking and sensational. (2) *National threat situation* was represented as a binary variable of the survey period. The period of 2013 was considered as the homeland security threat situation, coded as = 1, and the period of 2015 was the non-threat situation, coded as = 0. To check whether these two periods indeed resulted from the different threat situations, we asked respondents about their feeling of anxiety from the situation in each period (i.e., measured as 'situational anxiety'). (3) Government Internet surveillance effect was examined by using the variable *government Internet surveillance concerns (GISC)* adopted from Dinev, Hart, and Mullen (2008). Dinev et al. (2008)'s scale was designed for quantitative measuring of citizen assessment of government Internet surveillance. This variable was measured by multiple-item questions that asked

[1] As of 2017, the survey company (Dooit Survey) has a panel of five million potential respondents nationwide, from which 160,000 academic research and industry surveys have been conducted since the launch of the company. As one of the nationwide survey companies in South Korea, the company has in partnership with 30 major corporations (e.g., Samsung, POSCO, Korean Broadcasting System, etc.), six government and public organizations (e.g., Ministry of Employment and Labor, Korea Press Foundation, National Health Insurance Corporation), and 14 major universities.

Table 1
Survey instruments and reliability.

Variables	Question items	Inter-item reliability		
		All	Survey1	Survey 2
Situational anxiety	Overall, how fearful have you felt about the possible war with North Korea during the past few weeks? Overall, how serious has the issue of North Korea's nuclear weapon test been to you during the past few weeks?	0.72	0.76	0.70
Government internet surveillance concerns (GISC)	How much do you agree? "I'm concerned about the power the government has to wiretap Internet activities." How much do you agree? "I'm concerned that personal Internet accounts and database information (e.g. emails, shopping records, tracking my Internet surfing, etc.) will be more open to government security." How much do you agree? "I'm concerned about the government's ability to monitor Internet activities"	0.86	0.85	0.89
Rumor sharing intention	Below are the news stories found online right after North Korea's nuclear weapon test on February. Suppose that you read story online (3 stories). (1) North Korea received the Iranian government's financial support for nuclear test and had Iranian scientists visit to the test site. (2) US-ROK joint force is secretly planning to launch a preemptive attack if North Korean nuclear tests progress significantly. (3) A sexual assault to a South Korean woman by one of the U.S. military personnel was covered up due to the recent threat from North Korea. Would you re-post or share this story with others via online channels (e.g. social network sites such as Twitter and Facebook, blog, online forum, etc)?	–	–	–
Message belief	Do you believe this story conveys truth? (Yes/No)	–	–	–
Message anxiety	How anxious does this story make you when you read it?	0.71 (1)	0.72 (1)	0.70 (1)
	How serious do you think is the issue that this story contains?	0.75 (2) 0.72 (3)	0.77 (2) 0.75 (3)	0.71 (2) 0.67 (3)

Note: Blank cells are non-applicable; Items were asked by 7-point Likert scale except message belief.

respondents their perception regarding the legitimacy of government access to personal Internet accounts and database information, and the justifiability of government methods (i.e., wiretapping) to get online citizens' communication activities.

3.1.4.3. Control variables. The models controlled the effects of *demographic variables* including age, gender (female), education (1 = high school or less, 2 = college graduate, 3 = some post college, 4 = post-college graduate), and political orientation (1 = far liberal, 5 = far conservative).

3.2. Survey 2

3.2.1. Survey context: after North Korea apology in 2015

The second survey was conducted *after the settlement* of two-week tension between the two Koreas in August 2015. The tension arose from a landmine explosion that injured two South Korean soldiers patrolling the Demilitarized Zone (DMZ). The incident was followed by the South's accusation of North's planting the landmine, re-launching of loudspeaker propaganda broadcasts, and a few exchanges of fire between the two nations. On August 25, 2015, the two-week tension was resolved through a top-level meeting during which North Korea officially admitted and showed regret about their planting the landmine, and agreed with the South to reduce tension. Our survey was conducted a few days *after* the joint statement diffusing tensions was officially released.

3.2.2. Participants

Respondents were recruited from the same survey company's panel using the same sampling technique (gender and age-based quota sampling). The participants in the first survey were intentionally excluded from the recruitment. Among the 309 respondents who participated, those who were unaware of the North Korea's apology (and joint agreement to reduce tension) were eliminated due to possible misperception on the threat level. After the removal, a total of 261 responses were retained.

3.2.3. Rumor messages

The same rumor messages were replicated in the second survey. We fact-checked the three rumors after the first survey by tracking related news coverage and government statements. The Iran rumor was debunked by an official source, while the other two remained unsubstantiated. The Iran rumor was nonetheless replicated in the second survey along with the other two because it was unknown whether or not respondents were updated regarding the rumor's veracity. However, we advise readers to consider the possible bias in the Iran-rumor related results due to the official fact-check release between the two surveys.

3.2.4. Measurements

The same variables and the same questions were replicated for the second survey, except for a slight modification in wording for online rumor sharing intention: For this variable, we added the phrase, "Assume that you read this story right after the third North Korean nuclear experiment in Feb, 2013" to the original question. This phrase was added to minimize the systematic bias: this sentence intended to remind respondents of the North Korean threat in 2013, and let them answer the questions as if they were in a situation of threat. Evoking the threat situation helped collect the responses on rumor sharing intention in a more conservative manner than without doing it.

4. Results

4.1. Descriptive analyses

For the manipulation check whether each survey was indeed conducted in a different threat-level context, situational anxiety scores were compared. The mean scores were 4.52 (SD = 1.56) for Survey 1 (threat situation), and 3.92 (SD = 1.29) for Survey 2 (non-threat situation), t = 4.93, $p < 0.001$, indicating that the perceived threat level during Survey 1 was statistically higher than the threat level perceived during Survey 2.

Second, participant demographics and GISC were compared to ensure that the two surveys dealt with the same population. t-test of each of the demographic variables and GISC showed that none of them were statistically different between the two samples, confirming Survey 2 to be an appropriate replication without demographic biases.

Third, rumor message factors were compared. The belief level for Rumor 1 was significantly different, with more respondents in Survey 1

Table 2
Descriptive analysis: Comparison between Survey 1 and Survey 2.

Model	Combined		Survey 1		Survey 2		*t*-test	
N	572		311		261			
Variables	*M*	*SD*	*M*	*SD*	*M*	*SD*		
Message belief (1)	1.43	0.50	1.48	0.50	1.37	0.48	2.52	**
Message belief (2)	1.59	0.49	1.59	0.49	1.59	0.49	0.04	
Message belief (3)	1.40	0.49	1.42	0.49	1.38	0.49	0.94	
Message anxiety (1)	4.36	1.38	4.49	1.49	4.21	1.21	2.42	*
Message anxiety (2)	4.37	1.49	4.52	1.59	4.19	1.34	2.66	**
Message anxiety (3)	4.64	1.47	4.68	1.62	4.59	1.28	0.71	
Rumor sharing intention (1)	3.89	1.84	4.28	1.85	3.42	1.72	5.70	***
Rumor sharing intention (2)	3.95	1.82	4.29	1.83	3.55	1.73	4.94	***
Rumor sharing intention (3)	4.20	1.88	4.48	1.93	3.87	1.77	3.86	***
Situational anxiety	4.25	1.47	4.52	1.56	3.92	1.29	4.93	***
GISC	5.15	1.48	5.18	1.45	5.12	1.53	0.46	
Political orientation	3.06	0.61	3.05	0.59	3.08	0.64	0.76	
Education	1.77	0.63	1.74	0.62	1.81	0.65	1.31	
Gender	1.51	0.50	1.50	0.50	1.53	0.50	0.80	
Age	39.42	13.41	38.73	13.43	40.24	13.36	1.35	

Note: Rumor (1) = Iran involvement, Rumor (2) = military attack, Rumor (3) = sexual assault; GISC = Government internet surveillance concerns.
* $p < 0.05$.
** $p < 0.01$.
*** $p < 0.001$.

(48%) believing the rumor contained truth than in Survey 2 (37%), $t = 2.52, p < 0.01$. The difference could arise due to the fact-checking by official sources. Meanwhile, Rumor 2 and Rumor 3 did not show significant difference in message belief between the two surveys. Message anxiety was significantly higher for Rumor 1 and Rumor 2 in the first survey ($M = 4.49$, $SD = 1.49$ for Rumor 1, $M = 4.52$, $SD = 1.59$ for Rumor 2) than in the second survey ($M = 4.21$, $SD = 1.21$ for Rumor 1, $M = 4.19$, $SD = 1.34$ for Rumor 2) possibly due to the direct connection of the first two rumors to armed actions, $t = 2.42, p < 0.05$ for Rumor1; $t = 2.66, p < 0.01$ for Rumor 2. The anxiety induced from Rumor 3 was not significantly different between the two surveys.

Table 2 presents the descriptive comparison of variables between the two periods. In the meantime, the dependent variable, rumor sharing intention, was significantly higher in Survey 1 ($M = 4.28$, $SD = 1.85$ for Rumor 1, $M = 4.29$, $SD = 1.83$ for Rumor 2, $M = 4.48$, $SD = 1.93$ for Rumor 3) than in Survey 2 ($M = 3.42$, $SD = 1.72$ for Rumor 1, $M = 3.55$, $SD = 1.73$ for Rumor 2, $M = 3.87$, $SD = 1.77$ for Rumor 3) across all three rumors. Overall, descriptive statistics suggest that the responses during Survey 1 were not extremely sensitive to the situational threat and cyber-rumoring, but nonetheless higher than average. Similarly, the responses during Survey 2 were not anomalies in a situation of lower threat and cyber-rumoring. It is not surprising because the military tension has been a chronic, everyday political affair in South Korea for more than five decades. Nonetheless, Survey 1 was characterized by higher levels of situational threat and willingness of cyber-rumor sharing than during Survey 2 and such differences were statistically significant, meaning that the difference was not a random phenomenon. Meanwhile, the level of government Internet surveillance concerns was constant across both survey periods, suggesting that the surveillance concerns reflected South Korean citizens' stable assessment of the government policy over cyberspaces. Fig. 2 visualizes the response differences between the two surveys.

4.2. Results of each survey

4.2.1. Survey 1 (2013)

Our survey data structure exhibited within-respondent interdependency: A participant evaluated rumor-related variables three times (for each rumor story), resulting in rumor variables nested into individual respondents. That is, treating covariance as an independent structure may inflate the results. Generalized Estimating Equation (GEE) modeling allows a rumor message-level of analysis without neglecting within-subject dependency by estimating the within-subject covariance matrix as a part of the model (Burton, Gurrin, & Sly, 1998).

The GEE results indicated that, in Survey 1, three stories were *not* significantly different in estimating the sharing intention. Consistent with previous rumor research, message anxiety and message belief variables were the most significant factors in estimating cyber-rumor sharing intention: $b = 0.50$, $z = 14.58$, $p < 0.001$ for message anxiety; $b = -0.44$, $z = -4.73$, $p < 0.001$ for message belief, supporting H1a and H1b.

More importantly, cyber-rumor sharing was influenced not only by the message-related psychological factors but also by government internet surveillance concerns: GISC was *significantly and positively* associated with rumor sharing intention, $b = 0.22$, $z = 3.93$, $p < 0.001$, which respond to RQ1. Table 3 summarizes the results.

4.2.2. Survey 2 (2015)

Given the similar data structure with rumor variables nested within individual respondents, Survey 2 was also analyzed by the same analytic technique, GEE. In Survey 2, rumor sharing intention was disproportionately associated with different stories: Compared to Rumor 1, Rumors 2 and 3 were more likely to be shared, $b = 0.17$, $z = 2.40$, $p < 0.05$ for Rumor 2; and $b = 0.33$, $z = 3.81$, $p < 0.001$ for Rumor 2, possibly due to the debunking of Rumor 1. Akin to Survey 1, message anxiety was the most significant determinant of rumor sharing intention during Survey 2: $b = 0.37$, $z = 9.40$, $p < 0.001$. However, message belief was not significant.

An interesting result is that, in contrast to the positive effect of GISC on cyber-rumor sharing during Survey 1, the effect of GISC was *not significant* in Survey 2. This result implies that GISC is particularly more influential to cyber-rumoring when there is a national threat. The differential effect of GISC responds to RQ2. The results from Survey 2 are presented in parallel to Survey 1 in Table 3 above.

4.3. Pooled results

To better address the threat situational effect, another GEE modeling was conducted with the combined data of the two surveys. In this modeling, an independent variable "threat situation" represents the homeland threat contextual effect. The responses gathered during Survey 1 (threat situation, coded as 0), and responses from Survey 2 (non-threat situation, coded as 1). The results suggested that the threat situation was influential to cyber-rumor intention, increasing the willingness of sharing in time of threat (Survey 1) than a non-threat situation (Survey 2), $b = -0.64$, $z = -5.68$, $p < 0.001$.

Regarding GISC, the pooled model showed the positive main effect of GISC on cyber-rumor sharing intension, $b = 0.13$, $z = 3.27$, $p < 0.001$. Moreover, when interaction effect was added into the model, the effect of GISC *conditional to the homeland threat situation* was significant with a larger coefficient size than in the main effect model, $b = 0.21$, $z = 3.8$, $p < 0.001$. While this result confirms again that GISC was particularly influential during the threat situation, the threat situational effect did not necessarily moderate GISC effect on threat situational influence on cyber-rumor sharing in this combined model: the interaction effect was (marginally) non-significant, $b = -0.15$, $z = -1.99$, $p = 0.056$. The results are summarized in Table 3 above.

To gain more granular understanding, the OLS regression modeling was performed by separating each rumor (Table 4). The OLS resulted in

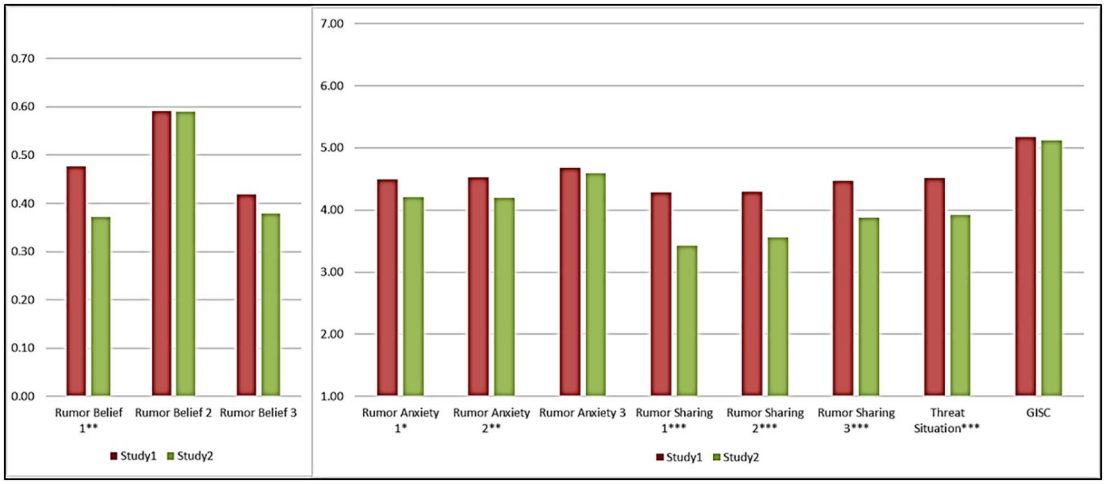

Fig. 2. Mean difference between Survey 1 and Survey 2 (Rumor belief scaled in 0–1 point).

a few interesting findings. First, the effects of message anxiety and threat situation were consistently significant across all three stories, validating the findings from the GEE modeling regarding H1b and H2. Second, message belief had a positive effect on the sharing of Rumor 1 and Rumor 3 but was not significant on Story 2, partially supporting H1a. Third, the main effect of GISC was significant only for Rumor 1. However, when the effect of GISC was *conditioned to the threat situation*, it had a positively effect on rumor sharing *across all stories*. These results make a strong case that GISC is particularly influential to facilitate cyber-rumor sharing during the homeland security threat situation. Lastly, GISC had a significant interaction with the treat situation in influencing rumor sharing intention for Rumor 3. Fig. 3 visualizes the moderating effect of threat situation on the relationship between GISC and the sharing intention of Rumor 3. To summarize, citizens who showed the low GISC revealed only a slight increase in rumor-sharing intention under the threat situations. However, citizens with high GISC became much more willing for rumor sharing under the threat situation in a disproportionate manner. Table 5 summarizes the modeling results from the various models.

5. Discussion: government internet surveillance, cyber-rumors, and homeland security

Cyber-rumors often become sources of discord between government and the public, known to be adversary to homeland security efforts. Some governments including South Korea are aware of the detrimental effects of cyber-rumoring, and adopt Internet surveillance program as a part of homeland security information management policy. However, the actual effectiveness of government Internet surveillance for mitigating cyber-rumoring in the general publics has been unclear due to its dual implications. On the one hand, it could be effective: government surveillance over cyberspaces may not only help detect adversarial actors but also facilitate self-censoring culture in the general publics. On the other hand, it could be counterproductive: surveillance creates a climate of distrust in civil society against government, which could facilitate citizens' anti-government cyber-rumoring.

The current study points to this paradox, and empirically addresses the effect of Internet surveillance on moderating citizens' cyber-rumoring tendency. Along with widely attested psychological variables—message belief and anxiety, and threat situational factor—we added government Internet surveillance concerns (GISC) as a societal factor of cyber-rumoring. GISC is a relevant variable for understanding cyber-rumoring tendency since cyber-rumors arise within a broader context of

Table 3
Results from GEE models.

Model	Separate models						Pooled models					
	Survey 1			Survey 2			Main			Interaction		
	b	C.I.		b	C.I.		Coef.	C.I.		Coef.	C.I.	
Threat situation							− 0.637***	− 0.857	− 0.417	− 0.635***	− 0.854	− 0.416
Rumor (2)	0.046	− 0.115	0.207	0.163*	0.024	0.302	0.107	− 0.003	0.217	0.112*	0.002	0.221
Rumor (3)	0.077	− 0.117	0.271	0.314***	0.147	0.481	0.182**	0.052	0.312	0.186**	0.056	0.316
Message belief	− 0.441***	− 0.625	− 0.258	− 0.124	− 0.280	0.032	− 0.285***	− 0.409	− 0.162	− 0.289***	− 0.412	− 0.165
Message anxiety	0.489***	0.422	0.555	0.365***	0.288	0.441	0.441***	0.390	0.492	0.445***	0.394	0.496
GISC	0.188***	0.093	0.282	0.061	− 0.066	0.187	0.127**	0.051	0.204	0.213***	0.103	0.323
Political orientation	0.231*	0.001	0.462	0.083	− 0.214	0.381	0.200*	0.017	0.383	0.166	− 0.019	0.351
Education	0.009	− 0.218	0.235	− 0.124	− 0.401	0.154	− 0.084	− 0.261	0.093	− 0.066	− 0.243	0.112
Gender	0.266	− 0.016	0.548	− 0.072	− 0.433	0.289	0.103	− 0.124	0.329	0.107	− 0.119	0.333
Age	− 0.007	− 0.017	0.003	− 0.001	− 0.014	0.013	− 0.003	− 0.011	0.006	− 0.003	− 0.012	0.005
Threat situation X GISC										− 0.152	− 0.295	0.004

Note: Threat situation = Threat (Survey1) as reference; Rumor (1) = Iran involvement (reference), Rumor (2) = military attack, Rumor (3) = sexual assault; GISC = Government Internet surveillance concerns; Conditional/Interaction model based on the mean-centered data.

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

Table 4
Results from the OLS models for each rumor.

	Rumor (1)				Rumor (2)				Rumor (3)			
	Beta	S.E.	t		Beta	S.E.	t		Beta	S.E.	t	
Main effect model												
Message belief	− 0.121	0.137	− 3.28	**	− 0.067	0.140	− 1.77		− 0.081	0.138	− 2.26	*
Message anxiety	0.392	0.051	10.30	***	0.405	0.047	10.61	***	0.503	0.048	13.25	***
Threat situation	− 0.206	0.137	− 5.57	***	− 0.155	0.135	− 4.21	***	− 0.147	0.130	− 4.27	***
GISC	0.087	0.047	2.29	*	0.069	0.047	1.82		0.067	0.047	1.81	
Age	− 0.003	0.005	− 0.09		− 0.010	0.005	− 0.26		− 0.019	0.005	− 0.52	
Gender	0.016	0.140	0.43		0.011	0.139	0.29		0.024	0.135	0.68	
Political orientation	0.053	0.114	1.40		0.106	0.113	2.81	**	0.039	0.108	1.12	
Education	0.003	0.109	0.07		− 0.080	0.108	− 2.13	*	− 0.007	0.105	− 0.21	
	$F(8563) = 24.37$, $p < 0.001$, Adj. $R^2 = 0.25$				$F(8563) = 23.61$, $p < 0.001$, Adj. $R^2 = 0.24$				$F(8563) = 36.32$, $p < 0.001$, Adj. $R^2 = 0.33$			
Interaction effect model												
Message belief	− 0.121	0.138	− 3.28	**	− 0.066	0.140	− 1.75		− 0.087	0.137	− 2.44	*
Message anxiety	0.392	0.051	10.30	***	0.407	0.047	10.67	***	0.504	0.048	13.35	***
Threat situation	− 0.206	0.137	− 5.57	***	− 0.155	0.135	− 4.21	***	− 0.147	0.129	− 4.3	***
GISC	0.116	0.064	2.26	*	0.112	0.063	2.2	*	0.154	0.062	3.16	**
Age	− 0.005	0.005	− 0.13		− 0.012	0.005	− 0.31		− 0.022	0.005	− 0.62	
Gender	0.017	0.140	0.44		0.011	0.139	0.29		0.025	0.134	0.7	
Political orientation	0.048	0.116	1.24		0.098	0.114	2.55	*	0.023	0.109	0.64	
Education	0.006	0.110	0.16		− 0.075	0.109	− 1.98	*	0.004	0.105	0.1	
Threat situation X GISC	− 0.043	0.092	− 0.83		− 0.065	0.092	− 1.26		− 0.132	0.088	− 2.73	**
	$F(9, 562) = 21.68$, $p < 0.001$, Adj. $R^2 = 0.25$.				$F(9, 562) = 21.18$, $p < 0.001$, Adj. $R^2 = 0.24$				$F(9, 562) = 33.48$, $p < 0.001$, Adj. $R^2 = 0.34$, Change in $R^2 = 0.009$, $p < 0.01$			

Note: Rumor (1) = Iran involvement (reference), Rumor (2) = military attack, Rumor (3) = sexual assault; GISC = Government internet surveillance concerns; All models are based on mean-centered data.
* $p < 0.05$.
** $p < 0.01$.
*** $p < 0.001$.

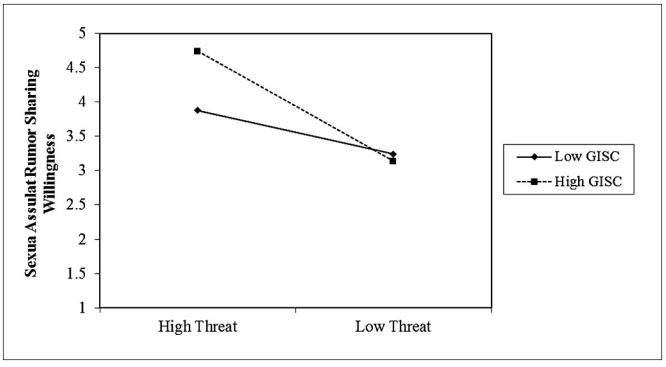

Fig. 3. Interaction effect between government Internet surveillance concerns (GISC) and threat situation (the sexual assault rumor).*High and low GIS were set based on the one standard deviation.

the nation's informational governance. The study's findings on psychological variables fell in line with previous findings of offline rumor studies, particularly revealing the influence of message anxiety and threat situational factors on increasing individual citizens' willingness for cyber-rumor sharing. Especially, the threat situational effect was consistently significant across all different models. Since few studies have been conducted under a societal-scale threat situation, the current study adds empirical evidence for citizens' susceptibility to cyber-rumors under nationwide threat situations such as the homeland security risk.

The central contribution of the study is to introduce government internet surveillance effect to cyber-rumor research. At the beginning of this paper, we mentioned that this project was launched with an initial anticipation to observe self-censoring effect on the rumor sharing intention among South Korean publics. This conjecture seemed germane to South Korea's information policy context where civil society has experienced several cases of free speech and privacy suppressions from government Internet surveillance. Contrary to the initial assumption, however, the findings confirmed the effect of GISC in *increasing* South Korean citizens' cyber-rumoring tendency. Especially, the aggravating effect of GISC was prominent during the homeland threat situation. These results imply the potential for surveillance-concerned citizens to rely on rumors or unorthodox sources of information to cope

Table 5
Summary of testing results.

Models	GEE			OLS Regression		
	Survey1	Survey2	Pooled	Rumor (1)	Rumor (2)	Rumor (3)
Message belief	Supported	NS	Supported	Supported	NS	Supported
Message anxiety	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**	**Supported**
Threat situation	–	–	**Supported**	**Supported**	**Supported**	**Supported**
GISC (Main)	Supported	NS	Supported	Supported	NS	NS
GISC (conditional to threat situation)	–	–	**Supported**	**Supported**	**Supported**	**Supported**
GISC x threat situation	–	–	NS	NS	NS	Supported

Note: Rumor (1) = Iran involvement, Rumor (2) = military attack, Rumor (3) = sexual assault; GISC = government Internet surveillance concerns; **Bold** = hypothesis supported across all tested models; blank cells are non-applicable; NS = not supported.

with cognitive uncertainty induced from the national threat situation.

Especially, the GISC's conditional and moderating effects were the most prominent for Rumor 3 about the military sexual assault rumor. This result is noteworthy because the sexual assault rumor was the *least* directly related to the saber-rattling incident itself, while it was the *most divisive and anti-government rumor* (the government position is pro-US military). The rumor had a potential to deepen the prejudice not about the enemy (North Korea) but about the ally (U.S.) that South Korean government needs to collaborate with for national defense. In other words, the results suggest heightened concerns about government Internet surveillance could assist the spread of malicious rumors that could thwart government's defense strategic efforts.

Overall, we interpret the findings related with GISC as a *distrust* effect on cyber-rumoring: the government Internet surveillance could induce citizens' distrust in government's informational integrity, which could subsequently cultivate disbelief in official sources of information (Reddick, Chatfield, & Jaramillo, 2015). Although there is no extant theory dedicated to explain this phenomenon, earlier scholarly remarks may give some guidance. According to Nissenbaum (2004), for example, citizens may evaluate the legitimacy of government Internet surveillance practice based on whether the practice preserves "informational norms" in cyberspaces that citizens anticipate to maintain (p.119). Citizens' concerns about government Internet surveillance could imply their discovery of government violating informational norms in cyberspaces. Bekkers, Edwards, and de Kool (2013) also contend that government monitoring of cyberspace needs to balance between instrumental goals and fundamental principles that citizens' value such as civil rights and procedural transparency. Therefore, citizens' perception of violated informational norms can diminish their faiths in government's overall integrity regarding its information policy. The distrust may then encourage citizens' belief in, and reliance on hearsays when they are in needs of information such as a national threat situation. This undesirable consequence of government Internet surveillance could be proposed as a 'distrust proposition' of cyber-rumoring.

While the current study cannot validate the distrust proposition, our findings offer preliminary insights for future research, with a few practical implications concerning government national security information policy. First, gaining citizens' faith in government's informational integrity is an important precondition for government to effectively manage cyber-rumors. Second, when implementing the Internet surveillance for the sake of seizing malicious rumormongers, government needs to reduce citizens' concerns by assuring reasonable motivations underlying the surveillance activities. Third, although citizens' lack of trust in government as an informational agent may not have visible impact on ordinary workings of government, government should be aware that citizens' distrust can weaponize cyber falsehood when the homeland security is under a threat. Government needs to be cautious about this latent power because the threat situation is the very moment when government-citizen collaboration is especially urgent (Lee, 2009).

6. Limitations and future directions

As a preliminary exploration, this study demonstrated the impact of government Internet surveillance concerns on citizens' cyber-rumor sharing intention. Based on the findings, we extended our discussion toward a 'distrust proposition' of cyber-rumoring. The current study, however, has several limitations to verify this proposition. Such limitations exist largely because testing the distrust effect was not an original plan at the onset of this project. Therefore, we invite future research to examine this proposition with more systematic modeling and theorization effort. For example, one of the important limitations in this study is that it did not include a variable that operationalizes citizen distrust in government in predicting cyber-rumor sharing intention. Consideration of a distrust-related variable could help probe the distrust effect as either an independent main effect or a mediating effect that links the government Internet surveillance concerns to cyber-rumor sharing intention. Future research is necessary to elaborate the distrust logic by delving into the method for measuring and analyzing the effect of citizen distrust on the process of cyber-rumoring.

Second, whereas one of the strengths of this study was to examine a real-world situational effect, this consideration at the same time became a limitation of the research design. Specifically, despite our attempt to eliminate ecological biases from the turmoil of Sewol ferry disaster in 2014—by conducting the second survey in the following year—the impact of Sewol incident on shaping citizen attitudes toward the government could have been too profound to be neglected. Moreover, the two-year gap between the two surveys resulted in the official refutation against one rumor story (the Iran rumor) before the second survey was conducted. The rumor correction could contaminate the survey responses if a participant was aware of this rumor's lifecycle. Future research may address this challenge by using realistic yet fictional rumor stories.

Also, this study considered only belief and message anxiety variables as message-level factors and demographic differences as control variables. Although belief and anxiety are the most widely confirmed determinants of rumor transmission, other variables such as personal involvement with message, trait anxiety, and the exposure to counter-rumor messages could further affect cyber-rumor sharing intention. The use of a binary scale for rumor belief, instead of an interval-scale item, also weakens the rigor of the analysis. Equally importantly, individual difference regarding their Internet use activities was not considered in this study. As much as the dependent variable was about cyber-rumor sharing, general activity on cyberspace could affect their tendency to engage with cyber-rumors. Future studies are recommended to consider respondents' Internet and social media use variables. Lastly, a manipulation check on anti-government sentiment of rumor stories could have enhanced generalizability of the study. Related to this, cultural contingencies could have some unique effects on our findings. South-North tension on the Korean peninsula has been a persistent cause of national insecurity, distinctive from acute events. We cannot tell the ways in which the nation's military history and other sociopolitical characteristics would affect the outcomes.

7. Concluding remarks

Overall, this study's findings highlight an aggravating impact of government Internet surveillance on citizen engagement with cyber-rumors. Under a national threat situation, citizens' attempt to manage their terrors can manifest in form of cyber-rumormongering. If citizens do not trust their government's informational integrity, cyber-rumoring could be anti-government, and become more detrimental to government information management efforts. While the current study focused on the military conflict situation, our findings resonate with other types of national security, social unrest, and public safety threat situations.

Meanwhile, we speculate that our findings could hold validity at some population levels. Certain minority groups could experience a self-censoring effect. Also, self-censoring effect may be particularly prevalent in non-democratic societies (e.g., North Korea), in which a turning point from self-censoring to distrust effect could occur amidst social unrest (e.g., political uprisings in Arab Spring). It will be an interesting future project to examine the boundary conditions under which distrust effect (or conversely self-censoring effect) occurs. As Landwehr (2016) articulates, "has the chilling effect of surveillance on free expression been studied systematically? … if [research] do not exist, they deserve study" (p. 30).

Acknowledgement

We would like to thank the editor and anonymous reviewers for providing very helpful comments. This research is funded in part by

NSF under grant nos. 1651475, 1724725 and #1651060.

References

Allport, G. W., & Postman, L. J. (1965). *The psychology of rumor*. New York: Russell & Russell.

Bekkers, V., Edwards, A., & de Kool, D. (2013). Social media monitoring: Responsive governance in the shadow of surveillance? *Government Information Quarterly*, *30*(4), 335–342.

Bergkvist, L., & Rossiter, J. R. (2007). The predictive validity of multiple-item versus single-item measures of the same constructs. *Journal of Marketing Research*, *44*(2), 175–184.

Bernardi, D. L., Cheong, P. H., Lundry, C., & Ruston, S. W. (2012). *Narrative landmines: Rumors, Islamist extremism, and the struggle for strategic influence*. New Jersey: Rutgers University Press.

Burton, P., Gurrin, L., & Sly, P. (1998). Extending the simple linear regression model to account for correlated responses: An introduction to generalized estimating equations and multilevel mixed modelling. *Statistics in Medicine*, *17*, 261–291.

Cho, D., & Kwon, K. H. (2015). The impacts of identity verification and disclosure of social cues on flaming in online user comments. *Computers in Human Behavior*, *51*, 363–372.

Christie, G. C. (1972). Government surveillance and individual freedom: A proposed statutory response to Laird v. Tatum and the broader problem of government surveillance of the individual. *NYUL Rev. 47*, 871–902.

Dalziel, G. (2013a). Rumors of terrorism: Social cognitive structures, collective sensemaking, and the emergence of rumor. In G. Dalziel (Ed.), *Rumor and communication in Asia in the internet age* (pp. 106–123). London: Routledge.

Dalziel, G. (2013b). Introduction. In G. Dalziel (Ed.), *Rumor and communication in Asia in the internet age* (pp. 1–19). London: Routledge.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98.

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. http://dx.doi.org/10.1016/j.giq.2017.02.007.

Deibert, R. J. (2003). Black code: Censorship, surveillance, and the militarisation of cyberspace. *Millennium*, *32*(3), 501–530. http://dx.doi.org/10.1177/03058298030320030801.

DiFonzo, N., & Bordia, P. (2007). Rumor, gossip, and urban legends. *Diogenes*, *54*(1), 19–35.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214–233.

Edy, J. A., & Risley-Baird, E. E. (2016). Rumor communities: The social dimensions of internet political misperceptions*. *Social Science Quarterly*, *97*(3), 588–602. http://dx.doi.org/10.1111/ssqu.12309.

Einwiller, S. A., & Kamis, M. A. (2009). Rumor has it: The moderating effect of identification on rumor impact and the effectiveness of rumor refutation. *Journal of Applied Social Psychology*, *38*(9), 2248–2272.

Fine, G. A. (2005). Rumor matters: An introductory essay. In G. A. Fine, & V. C. Heath (Eds.), *Rumor mills: The social impact of rumor and legend* (pp. 1–7). New Brunswick, NJ: Transaction Publisher.

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. London: Allen & Lane.

Freedom House (2016). Silencing the messenger: Communication apps under pressure. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2016.

Garrett, R. K. (2011). Troubling consequences of online political rumouring. *Human Communication Research*, *37*, 255–274.

Hubbard, R., Vetter, D. E., & Little, E. L. (1998). Replication in strategic management: Scientific testing for validity, generalizability, and usefulness. *Strategic Management Journal*, *19*(3), 243–254.

Jaeger, P. T., Bertot, J. C., & McClure, C. R. (2003). The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. *Government Information Quarterly*, *20*(3), 295–314.

Jung, K., & Park, H. W. (2014). Citizens' social media use and homeland security information policy: Some evidences from Twitter users during the 2013 North Korea nuclear test. *Government Information Quarterly*, *31*(4), 563–573.

Kimmel, A. J., & Keefer, R. (1991). Psychological correlates of the transmission and acceptance of rumors about AIDS. *Journal of Applied Social Psychology*, *21*(19), 1608–1628.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, *107*(2), 326–343. http://dx.doi.org/10.1017/S0003055413000014.

Knapp, R. (1944). A psychology of rumor. *The Public Opinion Quarterly*, *8*, 22–37.

Kwon, K. H., Bang, C., Egnoto, M., & Rao, H. R. (2016). Social media rumors as improvised public opinion: Semantic network analyses of Twitter discourses during Korean saber rattling 2013. *Asian Journal of Communication*. (Online First). http://dx.doi.org/10.1080/01292986.2015.1130157.

Kwon, K. H., & Cho, D. (2015). Swearing effects on citizen-to-citizen commenting online: A large-scale exploration of political vs. non-political online news sites. *Social Science Computer Review*. (Online first). http://dx.doi.org/10.1177/0894439315602664.

Kwon, K. H., Oh, O., Agrawal, M., & Rao, H. R. (2012). Audience gatekeeping in the Twitter service: An investigation of tweets about the 2009 Gaza conflict. *AIS Transactions on Human-Computer Interaction*, *4*(4), 212–229.

Landau, S. (2013). Making sense of Snowden: What's significant in the NSA surveillance revelations. *IEEE Security and Privacy*, *11*(4), 54–63.

Landwehr, C. (2016). Privacy research directions. *Communications of the ACM*, *59*(2), 29–31.

Lee, K. (2009). How the Hong Kong government lost the public trust in SARS: Insights for government communication in a health crisis. *Public Relations Review*, *35*(1), 74–76.

Leitner, J. (2009). Identifying the problem: Korea's initial experience with mandatory real name verification on Internet portals. *Journal of Korean Law*, *9*, 83–108.

Li, J., Vishwanath, A., & Rao, H. R. (2014). Retweeting the Fukushima nuclear radiation disaster. *Communications of the ACM*, *57*(1), 78–85.

Liberman, A., & Chaiken, S. (1991). Defensive processing of personally relevant health messages. *Personality and Social Psychology Bulletin*, *18*(6), 669–679.

Lyon, D. (2015). *Surveillance after Snowden*. Cambridge, UK: Polity.

Lyu, H. S. (2012). Internet policy in Korea: A preliminary framework for assigning moral and legal responsibility to agents in internet activities. *Government Information Quarterly*, *29*(3), 394–402.

Newell, B. C. (2014). Technopolicing, surveillance, and citizen oversight: A neorepublican theory of liberty and information control. *Government Information Quarterly*, *31*(3), 421–431.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*, 101–139.

Nissenbaum, H. (2015). *Respect for context as a benchmark for privacy online: What it is and isn't*. Cambridge, UK: Cambridge University Press.

Oh, O., Agrawal, M., & Rao, H. R. (2013). Community intelligence and social media services: A rumor theoretic analysis of tweets during social crises. *Management Information Systems Quarterly*, *37*(2), 407–426.

Pavone, V., & Degli Esposti, S. (2010). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science*, *21*(5), 556–572.

Pezzo, M. V., & Beckstead, J. W. (2006). A multilevel analysis of rumor transmission: Effects of anxiety and belief in two field experiments. *Basic and Applied Social Psychology*, *28*, 91–100.

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on national security agency surveillance programs: A multi-method approach. *Government Information Quarterly*, *32*(2), 129–141.

Rosnow, R. L. (1980). Psychology of rumor reconsidered. *Psychological Bulletin*, *87*(3), 578–591.

Rosnow, R. L., Esposito, J. L., & Gibney, L. (1988). Factors influencing rumor spreading: Replication and extension. *Language & Communication*, *8*(1), 29–42.

Shibutani, T. (1966). *Improvised news: A sociological study of rumor*. Indianapolis, IN: Bobbs-Merrill.

Shin, J., Jian, L., Driscoll, K., & Bar, F. (2016). Political rumoring on Twitter during the 2012 US presidential election: Rumor diffusion and correction. *New Media & Society*. http://dx.doi.org/10.1177/1461444816634054.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information system security policy violations. *MIS Quarterly*, *34*(3), 487–502.

Solomon, S., Greenberg, J., & Pyszczynski, T. (1991). A terror management theory of social behavior: The psychological functions of self-esteem and cultural worldviews. *Advances in Experimental Social Psychology*, *24*, 93–159. http://dx.doi.org/10.1016/S0065-2601(08)60328-7.

Srivasta, S. S., & Kurup, D. (2012). After rumours, northeast people flee Bangalore. The Hindu, from http://www.thehindu.com/news/national/karnataka/after-rumours-northeast-people-flee-bangalore/article3776549.ece.

Starbird, K., Maddock, J., Orand, M., Achterman, P., & Mason, R. M. (2014). Rumors, false flags, and digital vigilantes: Misinformation on Twitter after the 2013 Boston Marathon Bombing. *iConference 2014 Proceedings* (pp. 654–662). . http://dx.doi.org/10.9776/14308.

Sunstein, C. R. (2009). *On rumors: How falsehoods spread, why we believe them, what can be done*. New York, NY: Farrar, Straus, and Giroux.

Walker, C. J., & Beckerle, C. A. (1987). The effect of state anxiety on rumor transmission. *Journal of Social Behavior and Personality*, *2*(3), 353–360.

Wang, S. S., & Hong, J. (2010). Discourse behind the forbidden realm: Internet surveillance and its implications on China's blogosphere. *Telematics and Informatics*, *27*(1), 67–78. http://dx.doi.org/10.1016/j.tele.2009.03.004.

Wanous, J. P., Reichers, A. E., & Hudy, M. J. (1997). Overall job satisfaction: How good are single-item measures? *Journal of Applied Psychology*, *82*(2), 247–252.

You, J. (2015). The Cheonan incident and the declining freedom of expression in South Korea. *Asian Perspective*, *39*(2), 195–219. http://dx.doi.org/10.5555/0258-9184-39.2.195.

K. Hazel Kwon is an assistant professor in the Walter Cronkite School of Journalism and Mass Communication at Arizona State University.

H.R.Rao is the AT & T chair Prof of Information Systems and Cybersecurity at University of Texas At San Antonio. He has a courtesy appointment with Department of Computer Science.