Government Information Quarterly xxx (xxxx) xxx–xxx

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

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