Government Information Quarterly 31 (2014) 563–573

Contents lists available at ScienceDirect

Government Information Quarterly

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

Citizens' social media use and homeland security information policy: Some evidences from Twitter users during the 2013 North Korea nuclear test

Kyujin Jung [a], Han Woo Park [b,*]

[a] Dept. of Public Administration, University of North Texas, USA
[b] Dept. of Media & Communication, Yeungnam University, South Korea

ARTICLE INFO

Available online 26 September 2014

Keywords:
Homeland security
Risk communication
North Korea nuclear test
Social media use
Twitter networks

ABSTRACT

In the era of Web 2.0, managing risk communication on social networking sites has increasingly become crucial and complicated issues in the field of homeland security. The response to the 2013 nuclear test in North Korea was largely based on a coordinated effort by Korea's Ministry of Defense, the United Nations, and many countries from around the globe. By analyzing risk communication networks emerged from Twitter users for the period from January 30 to February 24, 2013, this study investigates the way in which citizens' risk communication is formulated through social media and how they transmit risk information in homeland security. Analysis results show the dynamic evolution of risk communication networks based on influential actors with critical information who played pivotal roles in distributing this information to other actors.

1. Introduction

As indicated in Beck (1992, 2008), rapid technological advances have led to a "risk society" in which the safety of the public has been overtaken by the risk derived from conflicts between religions, states, and organizations through the creation of diverse weapons of mass destruction (WMD) such as biological and nuclear weapons. After the United Nations Security Council's Resolution 2087 concerning North Korea on January 22, 2013, the country carried out its third nuclear test in Punggye-ri, Mantapsan, Hamkyeongbuk-do, on February 12, 2013. The international community, particularly East Asian countries, was shocked and expressed concern over threats to global security and safety by North Korea's continued nuclear program. In terms of crisis management, scholars and practitioners have increasingly highlighted the importance of networked actors' communication (FEMA, 2013; Purpura, 2007; Ressler, 2006), but little attention has been paid to citizens' social media use in risk communication in the context of homeland security.

Recent years have witnessed the great potential of social networking sites such as Twitter and Facebook as crucial communication tools for managing crises (Bird, Ling, & Haynes, 2011; Spong, 2011; Yates & Paquette, 2011), but few studies have examined the patterns of risk communication through social media during threats involving terrorist attacks. Because deficient risk communication may limit emergency responses and recovery efforts (Cole & Fellows, 2008), interorganizational and interpersonal communication plays a critical role in enhancing homeland security. In the field of risk communication through social media, both the situational theory of publics (STP) and the social amplification of risk framework (SARF) are used and discussed to predict and explain the behavior of the public on social media by focusing on a more in-depth picture of factors playing indispensable role in effective risk communication. In this study, the STP presents a theoretical framework for investigating how the public forms in the face of risk communication and when people are most likely to engage in such communication with others through social media (Aldoory, Kim, & Tindall, 2010; Aldoory & Sha, 2007; Binder, Scheufele, Brossard, & Gunther, 2011; Grunig, 2003), whereas the SARF focuses on the social context of various risks to shape different patterns of information diffusion by identifying the most critical actors facilitating effective risk communication on social media (Binder et al., 2011; Chung, 2011; Renn, 2011; Rogers, Amlot, Rubin, Wessely, & Krieger, 2007).

The primary objective of this study is to extend the STP and the SARF to the realm of risk communication on social media. To develop a theoretical framework for examining the dynamic evolution of risk communication on social media, the study considers North Korea's nuclear test in 2013 as the main research theme and employs longitudinal Twitter data collected in the U.S. and South Korea over the 24-day period of the nuclear test. Based on the theoretical framework derived from the STP and the SARF, the study is guided by the two research questions of (1) how citizens in the U.S. and South Korea formed different dynamically evolving patterns of risk communication on social media during the nuclear test and (2) how intermediary actors disseminating risk

* Corresponding author at: Dept of Media & Communication, Yeungnam University, 214-1, Dae-dong, Gyeongsan-si, Gyeongsangbuk-do 712-749, South Korea.
E-mail addresses: jkyujin@gmail.com (K. Jung), hanpark@ynu.ac.kr (H.W. Park).

http://dx.doi.org/10.1016/j.giq.2014.06.003
0740-624X/

information on social media facilitated information diffusion in different social contexts of South Korea and the U.S. The framework fundamentally posits that a serious homeland security threat would lead to the dynamic evolution of citizens' risk communication networks on social media (Wang, 2014) but have a limited impact on the clustering of subgroups because there may be no obvious actors coordinating crucial information even when more actors participate in and facilitate risk communication.

The next section presents the situational background of the nuclear test and then explores the concept of homeland security and its crisis management by comparing it with the field of crisis management. The theoretical framework derived from the STP and the SARF is presented in a comprehensible manner consisting macro, micro, and information diffusion perspectives. The study employs social network analysis (SNA) methods based on data collected from Twitter from January 30, 2013 (when North Korea promulgated martial law), to February 24, 2013 (12 days after the test). The results have important implications for crisis management in terms of the positive role played by the leading homeland security agency in designing and developing risk communication in the U.S. and South Korea, a topic generally overlooked in the literature.

2. Risk communication in homeland security

2.1. Risk communication in the homeland security information policy

Communication with the public is a critical but underdeveloped part of crisis management and homeland security (Bullock et al., 2006; Cole & Fellows, 2008; Pidgeon, 2012). In other words, communication in crisis management is limited to an activity for distributing important information before and after a terrorist threat to the public to prevent the anticipated loss. According to Deacker (2001), enhanced risk communication can reduce the risk derived from known or potential threats even when the risk cannot be completely eliminated. The U.S. Government Accountability Office (GAO) (2011) indicated that selecting the most efficient method for informing the public of risks is the key part of any crisis management in potential responses. Because providing timely and accurate information to the public can mitigate risks as well as reduce anticipated damage, risk communication can be an important tool for enhancing crisis management in homeland security.

Risk communication is defined as "an interactive process of exchange of information and opinion on risk among individuals, groups, and institutions" (The National Research Council, 1989, p. 12). In particular, the National Research Council (1995) highlighted that the process of risk communication is defined by the way in which individuals initially assess types and levels of a given risk and cope with the risk to reduce anticipated damage. According to The U.S. Public Health Service (1995), for example, risk communication is directly related to mentions and discussions in policymaking and decision-making processes concerning public issues that threaten communities' health or environment such as natural disasters and terrorist attacks. Through such processes, risk communication can facilitate individuals' behaviors to effectively respond to a catastrophic event by informing others of the need to be prepared for resultant risks.

Based on the homeland security information policy, risk communication with the public is formally composed of three basic stages: assessing threats, selecting methods, and distributing information (Deacker, 2001; Purpura, 2007). Before selecting the appropriate way to communicate with the public, the federal government and its agencies should identify various sources of threats that can result in death and property damage. This threat assessment evaluates the threat of miscommunication and a lack of information gathered by intelligence and law enforcement communities and also provides important support functions to facilitate appropriate decisions in a timely manner, thereby enabling them to capture emerging threats from terrorists (Purpura, 2007).

Based on assessed tools, the leading agency in homeland security should make decisions on the most efficient ways to distribute the threat of poor communication and information. Because the selection of communication methods is directly related to public awareness regarding the threat of terrorist attacks, the agency should identify appropriate ways to effectively inform the public instead of relying on various fragmented communication channels. This administrative fragmentation often limits the ability of certain marginalized groups to gain access to and interpret information.

Finally, the leading agency should distribute appropriate information in a timely manner and consistently update it through various channels. Any distributed information should not be too general or abstract to prevent unnecessary confusion. By providing too much information without considering its main effect regarding potential threats on public awareness, the leading agency may not successfully reach certain marginalized groups. Groups such as non-English-speaking communities tend to be less aware of potential threats and the best ways to deal with them.

However, many scholars have indicated that governments and agencies may not recognize the challenges involved in administering risk communication (Cole & Fellows, 2008; Pidgeon, 2012; Purpura, 2007). Although many studies have focused on risk communication, few have explored the importance of crisis management in the context of homeland security. For example, few has examined the critical aspects of managing risks such as ways to efficiently plan for homeland security and the most cost-effective technique for planning organizational continuance, that is, actions that must be taken before and after the loss to ensure the continuation of an organization (Purpura, 2007). Based on Richelson's (2006) book "Spying on the Bomb: American Nuclear Intelligence from Nazi Germany to Iran and North Korea," Chapman (2008) indicated that providing more detailed information on how difficult it is for U.S. citizens can strengthen positive aspects of risk communication on social media, although U.S. government agencies monitor other countries' WMD development and seek to protect citizens from the spread of nuclear weapons.

2.2. Social media use in risk communication in the context of homeland security

Social media can be defined as a set of "applications built on Web 2.0 technologies that are internet-based and designated to promote the content generation by the users and to facilitate the sharing and diffusion of information through social linking and interactions" (Chun & Reyes, 2012, p. 441; O'Leary, 2007). Web 2.0 technologies allow social media services such as Twitter, Facebook, YouTube, LinkedIn, and FourSquare to build platforms not only to freely connect individuals but also to facilitate efficient information sharing between them. As a case of social media use in the field of crisis management, an individual user can join Twitter and follow government agencies such as the Federal Emergency Management Agency (e.g., @fema and @ReadydotGov) and the U.S. Department of Homeland Security (e.g., @DHSgov and @citizen_corps). By communicating with such an agency during a catastrophic event, individual users can not only obtain crucial information such as assessed risks and shelter locations but also communicate with their friends and other subgroup members by transmitting information derived from the agency on Twitter.

The application and use of social media in crisis management have shed some important light on the behavior of the public, including the types of information sought by the public before, during, and after a threat. By considering the case of the 2010 Haitian earthquake, Yates and Paquette (2011) illustrated that in crisis communication management, social media can effectively influence the assessment of knowledge and the process of sharing and disseminating information. Bird et al. (2011) suggested that the use of social media such as Facebook and Twitter during the Queensland and Victorian floods played an important role in disseminating information as well as in providing information sources for informal communities that were not previously accessible. In practice,