Misuse of Information Technologies and Reliability of Information in New Media during Emergencies

Salvatore Scifo
Maltepe University, Turkey

Lemi Baruh
Koç University, Turkey

Hayley Watson
Trilateral Research and Consulting, UK

INTRODUCTION

In a recent commentary of the use of social media during a disaster, Meier, (2013, online) has argued that "disaster-affected crowds are increasingly 'digital crowds'… that is, both a source and consumer of that digital information." Both response organizations and members of the public are turning to new media information technologies to communicate information and coordinate action. For instance, in the aftermath of the Haiti earthquake, at a time when much of the communication infrastructure was inoperable or destroyed, collaboration between Ushahidi, In STEDD and others helped create an SMS system that enabled the public to use a single SMS short code to report incidents. These messages were then sorted and geolocated by volunteers via online crowdsourcing platforms (Nelson, Steckler, & Stamberger, 2011). Recent years have also shown that during political crises (e.g., the Arab Spring), social media, mobile technologies, and networks may play a crucial role in the diffusion of a movements ideas, mobilizing protestors, and exposing government misconduct (Cammaerts, 2013; Castells, 2012).

Despite information communication technologies' (ICT) potential as a tool that can assist emergency response and act as a catalyst of social movements, their improper use remains an important challenge in emergency communications. Drawing upon our current research in an EU funded project COSMIC, this article aims to provide an overview of the types and effects of improper use of ICTs and the diffusion of misinformation during emergencies, including political crises. This article will also consider the state of the art in managing misuse of ICTs during crises.

BACKGROUND

According to Hermann (1963), there are three distinguishable features that separate a "crisis" from other ill-fated occurrences: surprise, threat, and a short response time. These elements relate to a sudden change from the norm, where the everyday workings of a community are disrupted and subsequently require a response. Within this article, when discussing the term "crisis" we will also utilize (interchangeably) the term "disaster," as seen, for instance, in the 2010 "EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (European Commission, 2010). A disaster is a "social phenomena"; a storm for instance, is not a disaster, it is the social effects of the storm on the social system that causes it to be classified and understood as a disaster. An event might be classified as a disaster according to the number of systems damaged, citizens injured or displaced.

As stated by the International Telecommunications Union (ITU, 2005), communication is a critical component of preparing for, responding to, and recovering from crises. The tools available to those involved in responding to, as well as those caught up in a crisis, are no longer limited to the use of conventional telecommunications technologies, such as the telephone or radio, but have expanded to a host of

DOI: 10.4018/978-1-4666-5888-2.ch408

new media applications. New media applications are able to perform a range of functionalities, including: enabling one-way communication, facilitating two-way communication, enabling people to request/offer assistance, relay information, assist with campaigning activities, and, crucially, to enable individuals/groups to organize (Watson et al., 2013).

At the same time, the increased use of ICT and social media creates new challenges pertaining to both 1) misutilization of ICT technologies; and 2) misinformation/disinformation. Both of these categories may intentionally or unintentionally impede emergency response and/or put individuals and communities in danger. Accordingly, the following section will focus on these two types of misuse of ICTs and their potential impact on crisis response. Subsequently, by drawing on four case studies, we will examine the ways in which misuse of ICTs can be managed by authorities and the public. Case studies include:

- **Haiti Earthquake (2010):** Measuring 7.0, the earthquake killed at least 100,000 people, 300,000 were injured and 1.5 million were left without shelter (O'Connor, 2012).
- **Hurricane Sandy, USA (2012):** The hurricane, which hit the eastern coast of the United States, resulted in 72 direct deaths and 75 indirect. Damage caused by the hurricane is estimated to have cost at least $50 billion (Sullivan & Uccellini, 2013).
- **The Boston Marathon Bombings, USA (2013):** The attacks involved the detonation of two devices. Three people were killed and 264 runners and spectators were injured (Kotz, 2013).
- **Occupy Taksim, Turkey (2013):** Following the violent eviction of a small sit-in protest against a redevelopment project in Taksim Square area on May 28th, 2013, the protests quickly spread around Turkey, resulting in violent clashes between the protestors and the police, 11 fatalities, and thousands of injuries ("Turkish police admits suicides," 2013).

TYPES AND EFFECTS OF MISUSE OF INFORMATION TECHNOLOGIES

Misuse of ICT

The case studies revealed that a frequently occurring problem in the use of ICTs during emergencies concerns redundancies created by the lack of interoperability of systems. For example, in the early days of response efforts to the Haiti earthquake, a multitude of systems were set up for registering victims and missing people. However, as Stauffacher et al. (2011) report, even after the establishment of a standard-based repository by Google, agencies failed to share information with each other, leading to redundancies in capacity use, duplication of information, and the fragmentation of data. The experience from the events in Haiti is but one example of how various cultural, social, technical and economic factors may lead to ineffcient utilization of ICTS and consequently, coordination efforts. According to Nelson et al. (2011), these include but are not limited to; local service providers resisting ICT equipment brought by early respondents and intra-organizational competition disrupting the interoperability of technologies.

Our case studies have shown that social media may also lead to inefficiencies in emergency response when the public uses social media for a specific communicative purpose, despite the existence of more established communication technologies (with better procedures already in place) for that purpose. This was evident during Hurricane Sandy, when citizens tweeted calls for help, rather than using emergency phone lines, which were reportedly functioning ("Lessons learned," 2013). In such cases, there remains a risk that this type of use of social media, particularly when response teams are not prepared for it, may result in existing resources being strained, which can then reduce the efficiency with which assistance is delivered to citizens.

While the types of misuses of ICTs described above can be characterized as "unintended" (i.e., the purpose was not to create the resulting negative effect), in other situations, particularly during political crises, ICTs may purposefully be misappropriated. In such cases, stakeholders including government authorities, protestors, other members of the public (bystanders), and the media may be variously positioned as either the agent of misappropriation or its target.