Inf Syst Front (2011) 13:33–43
DOI 10.1007/s10796-010-9275-8

Information control and terrorism: Tracking the Mumbai terrorist attack through twitter

Onook Oh · Manish Agrawal · H. Raghav Rao

Published online: 25 September 2010

Abstract This paper analyzes the role of situational information as an antecedent of terrorists' opportunistic decision making in the volatile and extreme environment of the Mumbai terrorist attack. We especially focus on how Mumbai terrorists monitored and utilized situational information to mount attacks against civilians. Situational information which was broadcast through live media and Twitter contributed to the terrorists' decision making process and, as a result, increased the effectiveness of hand-held weapons to accomplish their terrorist goal. By utilizing a framework drawn from Situation Awareness (SA) theory, this paper aims to (1) analyze the content of Twitter postings of the Mumbai terror incident, (2) expose the vulnerabilities of Twitter as a participatory emergency reporting system in the terrorism context, and (3), based on the content analysis of Twitter postings, we suggest a conceptual framework for analyzing information control in the context of terrorism.

Keywords Mumbai terrorist attack · Twitter · Information control · Situation awareness

O. Oh (✉) · H. R. Rao
Management Science and Systems, School of Management,
University at Buffalo,
325 Jacobs, Management Center,
Buffalo, NY 14260-4000, USA
e-mail: onookoh@buffalo.edu

H. R. Rao
e-mail: mgmtrao@buffalo.edu

M. Agrawal
College of Business, University of South Florida,
CIS 1040, 4202 E. Fowler Ave,
Tampa, FL 33620-7800, USA
e-mail: magrawal@coba.usf.edu

1 Introduction

On November 26, 2008, terrorists mounted multiple attacks on Mumbai, resulting in arguably the worst terrorist incident in the history of India. According to the analysis of B. Raman, a former head of the Counterterrorism Division of the Research & Analysis Wing (R&AW) in India, the Mumbai terror attack was "the first mass casualty terrorism against innocent civilians, using hand-held weapons" in India (Indian Ministry of External Affairs 2009). His analysis implies that the use of hand-held weapons in the Mumbai terror incident enabled the attackers to convey their political agenda through the mainstream media. He argues that, given the preference of traditional anti-Indian terrorists for "timed or remotely controlled improvised explosive devices (IEDs)," the exploitation of hand-held weapons against civilians is indicative of a tactical shift in terrorist strategy—IEDs tend to rain indiscriminate blows on target areas in a short period of time such that it is not effective enough to send their messages about whom they intend to kill for what political agenda. Furthermore, because the visual impact that can be created by IEDs lasts at best one or two hours, the duration of media coverage is much shorter than for hand-held weapon attacks. Raman's main point is that, compared to the traditional IED attacks, the hand-held weapons strategy employed by Mumbai terrorists were more effective in conveying their political message vividly through media over a long duration, almost 60 hours.

Raman's analysis provides insight to consider Mumbai terror in terms of the triadic dynamics of (1) communication media including TV and Web, (2) attackers' synchronous monitoring of live media and Web and collection of situation information and, (3) use of the collected situation information for opportunistic decision making in terrorist action. Although the focus of Raman's analysis is not about how Mumbai terrorists used public or social media to their

advantage, a close reading of terrorists' phone conversations intercepted by the Indian government shows that the terrorist group collected situational information on the fly through live media and websites. They opportunistically utilized such information to make decisions of where and how to mount their attacks, and whom to kill with precision. That is, the remote handler's synchronous process of (1) monitoring of live media and websites, (2) collection of situational information on Mumbai under terrorist operation, (3) opportunistic decision making, and (4) delivery of action commands to onsite terrorist commandos not only enhanced the effectiveness of hand-held weapons but also facilitated the precise attack.

This paper analyzes the role of situation assessment process as an antecedent of terrorists' opportunistic decision making in the volatile and extreme environment of the Mumbai terrorist attack. The main argument of this paper is that the situational information which was broadcast through live media and Twitter contributed to the terrorists' decision making process and, as a result, it enhanced the effectiveness of hand-held weapons to accomplish their terrorist goal. We show that considerable amount of situational information was relayed to mainstream media via Twitter. To show that, we carry out content analysis of Tweets, and present that Twitter played a significant role in relaying situational information of Mumbai terrorist attack to the local and global mainstream media in an uncontrolled ad hoc way.

Through a review of cyber terrorism literatures, we identify critical issues caused by mobile and participatory social media, Twitter, in the terrorism context. By utilizing Information Warfare (IW) literature and Situation Awareness (SA) theory, this paper aims to (1) analyze the content of Twitter postings of the Mumbai terror incident, and (2) expose the vulnerabilities of Twitter as a participatory emergency reporting system in the terrorism context. An important finding is that unregulated real time Twitter postings can contribute to increase the level of situation awareness for terrorist group to make their attack decision. This paper presents practical implication of our findings for anti-terrorism policy makers and anti-terrorism security forces. After that, this paper proposes a research agenda for the design of Web 2.0 based participatory emergency reporting systems in terrorism context. This paper concludes that such systems need to incorporate information control mechanisms to deter or prevent the decision making of terrorists.

2 Prior literature

2.1 Cyber terrorism

This section describes previous research on cyber terrorism, particularly focusing on terrorism research which investigate how and why terrorists use websites. Terrorism researches dealing with terrorists' uses of website seem to center around two approaches: content analysis of terrorists' web documents (Tsfati and Weimann 2002; Weimann 2004; Denning 2009; Anderson 2003) and explication of terrorists' web technologies in supporting communication, interaction, and presentation (Qin et al. 2007).

In terms of content analysis, the plethora of research pronounces common findings. For instance, since the 9/11 terrorist attacks, terrorist organizations have gone through fundamental changes by actively adopting Internet for various reasons (Anderson 2003). According to Ariely (2008), similar to the organizations of the post-industrial age, terrorist groups have transformed toward "knowledge-centric" "networked organizations" to leverage information technology to achieve their goals with efficiency and innovation. In this frame, terrorist group members are analogous to knowledge workers. As is the knowledge organization, terrorist groups actively take advantage of the global Internet infrastructure to publicize political agenda, collect data on targets to attack, recruit supporters, exchange ideas, raise funds, transact or launder money, share terrorist manuals, and train terrorist members (Tsfati and Weimann 2002; Weimann 2004; Denning 2009).

An interesting research by Qin et al. (2007) supports the findings on how and why terrorists use websites. This research argues that, while terrorist and extremist groups' web knowledge is comparable with that of the US governement agencies, their use of multimedia, online forums, and chat rooms are much more sophisticated than that of US government's websites. This finding indicates that terrorist groups are employing web technolgies very actively to deliver their political propaganda with rich media (such as graphics or multimedia), to recruit potential terrorists and coordinate terrorist action (through chat room), to train terrorist members (through interactive web forum), to share or transit secrete manuals to concoct chemical or explosive bombs (through exchange of steganography or ciphered files).

However, so far, the research has not taken into consideration Web 2.0 based mobile social media such as Twitter and mobile phone, which enable instantaneous information exchange and communication on the road at group level. Given Gartner's predictions that (1) "within five years, 70% of collaboration and communications application […] will be modeled after user experience lessons from smartphone collaboration applications," and (2) "by 2012, over 50% of enterprises will use activity streams that include microblogging," extreme mobile device exchanging real time information of activity streams is supposed to cause unprecedented challenges in anti-terrorism efforts (Gartner 2010). For instance, the US army intelligence report includes Twitter as a potential terrorist

tool that can be adversely used by terrorist groups to coordinate precise attack by sharing real time situational information on the move (Shachtman 2008; Siegler 2008). They express concerns that Twitter can be a dangerous terrorist tool, especially when it is used in combination with Global Positioning System (GPS), voice-changing software, and mobile cellular phone. One of many virtual scenarios included in the report (Shachtman 2008) is as follows:

> "Scenario 2: Terrorist operative 'A' has a mobile phone for Tweet messaging and for taking images. Operative 'A' also has a separate mobile phone that is actually an explosive and/or a suicide vest for remote detonation. Terrorist operative 'B' has the detonator and a mobile to view A's Tweets and images. This may allow 'B' to select the precise moment of remote detonation based on near real time movement and imagery that is being sent by 'A'" (Shachtman 2008).

This scenario is imaginary. However, it implies a significantly different dimension from those identified from previous studies on terrorists' usage of web technologies. As Twitter is a web 2.0 based social media that is compatible with 140 character-based mobile texting devices, information exchange or sharing is not tied to wired computers or laptops. That is, Twitter enables coordination of terrorist action on the move based on the exchange of real time situational information at group level. Borrowing Ariel's (2008) expression, sharing of real time situational information on the move can enable the "sophisticated usage of the most primitive weapons".

This scenario has surprising similarity, although not exactly same, with the Mumbai terrorist attack, which will be detailed later in this paper in the content analysis section. In other words, the effectiveness of primitive hand-held weapons had been maximized when the terrorist groups' attack decision was coordinated with the exchange of real time situational information on the move through satellite phone between remote handlers in Pakistan and field attackers in Mumbai. Mumbai Terrorist attack shows that the exchange of up-to-date situation information can enable the "sophisticated usage of the most primitive weapons" to inflict harm against civilians. In this regard, anti-terrorist operations to suppress terrorism are an example of information war to maintain informational superiority between security forces and terrorist group.

2.2 Information Warfare (IW)

In the warfare situation, informational superiority operates as necessary means to achieve the end of suppressing the adversary. In this means-end framework, the nature of information tends to be tactical, situational or sometimes deceptive. The transformative nature of information is attributable to the frequent change of situation in warfare state: e.g., (1) the enemy constantly competes with allies to stay in a state of information superiority, and (2) the battlefield is filled with uncertainty and complexity under extreme conditions. Therefore, information control in battlefield operation is not necessarily based on factual data. Rather, in the warfare situation, information is an element "to be disseminated in a controlled fashion and, if necessary, to be created at will" in order to gain the information superiority over opponent (Hutchinson 2006). That is, since the warfield is filled with high level of uncertainties, both allies and adversaries need frequent updates and exchanges of situational information to maintain the position of information superiority.

According to the Chairman of the Joint Chiefs of Staff instruction (CJCSI) Number 3210.01 of 1996, IW is defined as:

> [A]ctions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems while defending one's own information, information-based processes, and information systems (Haeni 1997).

This directive presumes the earning of information superiority as a necessary condition for decision making in the war state. At the operational level, the goal of IW is to stymie the adversary's decision making and protect one's ally through various means of information control. The definitions of IW are similar to Situation Awareness (SA) theory in that the military action is preceded sequentially by the situation awareness and then decision making (Endsley 1995a). This temporal process of SA as an antecedent of decision-making and military action will be detailed in the next section.

3 Analysing the Mumbai terrorist event

To analyze Twitter content of Mumbai terrorist attack, we expand IW concept to information control. In this paper, information control is defined as a mean to maintain information superiority by deterring or preventing terrorists' decision making such that it contributes to allies' operations of suppressing terrorist action. Conversely, the failure of information control creates a situation where terrorists gain information superiority over allies such that they can mount precise attacks to bring about detrimental harm against the public. Therefore, we approach information control in terrorism as a strategically essential antecedent to stymie or minimize terrorists' gaining of situation awareness information and suppress the terrorist action.

Web 2.0, which is characterized as an open participatory or collaborative web platform (McAfee 2006), is a rapidly

shifting the mode of communication. Collaborative social reporting media, Twitter, spreads the notion that the maintenance of a symbiotic relationship between the public and government is essential to conduct a successful operation in extreme events (Lee 2002). However, our content analysis of Twitter in the Mumbai terror event discloses many unexpected problems as a participatory emergency reporting system. To understand these problems, SA theory is utilized to analyze the Mumbai Tweeter page from the terrorist perspective.

3.1 Situation awareness: Terrorist perspective

This section starts with an assumption that "the key to success in conflict is to operate within the opponent's decision cycle" (Taipale 2005). In this regard, Situation Awareness (SA) theory is important to understand the decision making process of terrorists. SA theory has been developed from and applied to the military discipline, this paper uses SA theory to analyze the opportunistic (but highly calculated) decision making process of Mumbai terrorists. SA theory specifies situation assessment as three distinct cognitive processes for gaining information superiority and positions SA as a critical antecedent of decision making for goal achievement.

Fundamentally, "situation awareness is understanding the state of environment" (Endsley 1995b). It provides the foundation for decision making followed by action in the operation of complex task. This model assumes that the higher level of SA is likely to produce better decision making followed by better performance, that is, better action. Endsley specifies SA as three distinct levels of cognitive processes as shown in Fig. 1.

At level one, an actor "perceives" diverse relevant information from dynamically changing external environments. At this level, understanding of situation is not formed yet. At best, it recognizes the relevance of situation for her/his goal achievement. At level two, the relevant information pieces are integrated into meaningful and understandable forms in conjunction with an actor's goal. Finally, at level three, the integrated meaning and understanding are projected into the future to predict the future state or event after the action (Endsley 1995b). Once the information of the external situation is processed from perception through comprehension to projection, calculated decision making follows to take certain action. In the process of SA, from level one to level three, the perception, comprehension, and projection of situational information are contingent upon the goal which an actor intends to achieve. That is, the actor's goal operates as a driving force to assess and decide the relevance, meaningfulness, and projection of situational information (Endsley 1995a).

The important point here is that Mumbai terrorist group also made an effort not only to maintain their information superiority, but to obtain up-to-date situational information by systematically monitoring mainstream media and websites. Once they obtained the situational information, they filtered it through the interpretive scheme of their political goals to decide the terrorist action to take. The process of Mumbai terrorist group's situation assessment process is detailed in the following case section.

3.2 Case study: Mumbai terrorist incident

SA theory brings insight to analyze Mumbai terrorists' decision making process for terrorist action in conjunction with their political goal. Raman suggests that the Mumbai terrorist group had three point political agendas to accomplish: (1) an anti-India agenda, (2) an anti-Israel and anti-Jewish agenda, and (3) an anti-US and anti-Nato agenda (Raman 2009). He believes that an anti-Indian agenda was designed to "create fears in the minds of foreign businessmen about the security of life and property in India and in the minds of the Indian public about the competence of the Indian security agencies to protect them." To accomplish these goals, the terrorists targeted the two luxury hotels of Taj and Oberoi Trident where many foreign businessmen stayed, and also targeted many Indian civilians in public places such as the railway station. For the anti-Israel and anti-Jewish agenda, Raman suggests that the terrorist group's objective was in line with anti-Israel and anti-Jewish agenda of Al Qaeda terrorist group. To accomplish this political agenda, the terrorists attacked the Nariman House which was used as a Jewish Center building. For the anti-US and anti-NATO agenda, Raman maintains that the Mumbai terrorist groups also followed the causes of Al Qaeda and the Afghan Taliban. As an evidence of his analysis for three political agenda of Mumbai terrorist group, he presents that "Of the

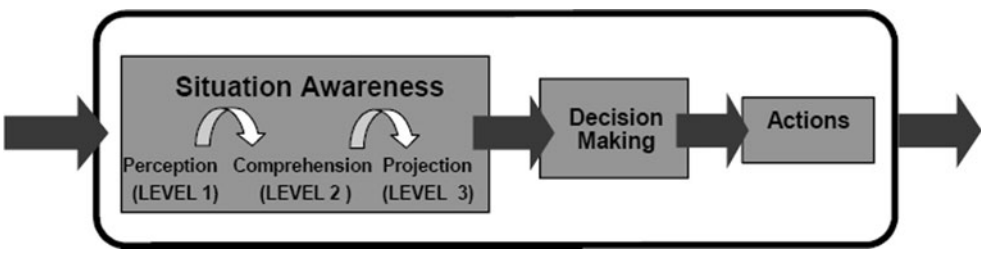

Fig. 1 Model of situation awareness levels and decision-action process (Strater et al. 2001)

25 foreigners killed, nine were either Israelis or Jewish persons, 12 were from countries which have contributed troops to the NATO in Afghanistan and four were from other countries. Nationals of European countries, which are not participating in the war against terrorism in Afghanistan, were not targeted" (Raman 2009).

In pursuit of these three political goals, an analysis of satellite phone conversations between terrorist commandos in Mumbai and remote handlers in Pakistan shows that the remote handlers in Pakistan were monitoring the situation in Mumbai through live media, and delivered specific and situational attack commands through satellite phones to field terrorists in Mumbai. For instance, the remote handler reminds one of his field terrorists that "Everything is being recorded by the media," and orders him to "Inflict the maximum damage. Keep fighting. Don't be taken alive" so that their tenacious terrorist action is broadcasted (Indian Ministry of External Affairs 2009).

Another phone conversation between a terrorist in Nariman House and a remote handler named Wassi presents the "situation assessment" process through monitoring of live media.

> Wassi: Keep in mind that the hostages are of use only as long as you do not come under fire because of their safety. If you are still threatened, then don't saddle yourself with the burden of the hostages, immediately kill them.
>
> Receiver: Yes, we shall do accordingly, God willing.
> Wassi: The Army claims to have done the work without any hostage being harmed. Another thing; Israel has made a request through diplomatic channels to save the hostages. If the hostages are killed, it will spoil relations between India and Israel.
>
> Receiver: So be it, God willing.

The remote handlers in Pakistan perceive (level one of SA) through live media that Israelis are in the Jewish Center without being harmed. Next, he comprehends (level two of SA) situation by integrating the facts about Israelis being taken hostage in the building and Israel government's diplomatic effort to save the Israelis hostages. Lastly, he predicts (level three of SA) that killing Israeli hostages will disrupt the diplomatic relations of India and Israel, which is their anti-Israel political goal.

From the IW perspective, this conversation shows that Indian government failed in information control. In other words, the Indian government did not need to disclose the information that Israel government requested to save the Israeli hostages. This unnecessary information brought information superiority to the Mumbai terrorist group, and they were able to use this information to maintain high level of SA. Eventually, combined with their three political agendas, the high level of SA led to effective and dynamic decision making to mount precise terrorist actions against civilians even in the extreme condition. One important point is that uncontrolled media aided remote handlers to sustain high level of SA, which led to their dynamic and highly calculated decision making to mount a precise attack against Jewish hostages.

The phone conversation provides evidence that the Mumbai terrorist groups understood the value of up-to-date situation information during the terrorist operation. They tried hard not to lose their information superiority to the Indian Anti Terrorist Squad (ATS) and National Security Guard (NSG). They understood that the loss of information superiority can compromise their operational goal. The following phone conversation between a remote handler in Pakistan and a field attacker in the Taj hotel shows terrorist's effort to maintain information superiority over Indian security forces:

> Handler: See, the media is saying that you guys are now in room no. 360 or 361. How did they come to know the room you guys are in?...Is there a camera installed there? Switch off all the lights…If you spot a camera, fire on it…see, they should not know at any cost how many of you are in the hotel, what condition you are in, where you are, things like that…these will compromise your security and also our operation […]
>
> Terrorist: I don't know how it happened…I can't see a camera anywhere (Khetan 2009).[1]

Another phone conversation shows that the terrorists group used the web search engine to increase their decision making quality by employing the search engine as a complement to live TV which does not provide detailed information of specific hostages. For instance, to make a decision if they need to kill a hostage who was residing in the Taj hotel, a field attacker reported the identity of a hostage to the remote controller, and a remote controller used a search engine to obtain the detailed information about him:

> Terrorist: He is saying his full name is K.R. Ramamoorthy.
>
> Handler: K.R. Ramamoorthy. Who is he? … A designer … A professor … Yes, yes, I got it …[The caller was doing an internet search on the name, and a results showed up a picture of Ramamoorthy] … Okay, is he wearing glasses? [The caller wanted to match the image on his computer with the man before the terrorists.]

[1] A documentary of Mumbai terror shows how remote handlers in Pakistan controlled field attackers in Mumbai through satellite phone by monitoring live TV. The video is available at: http://www.liveleak.com/view?i=1e4_1246490858 (Last accessed November 12th, 2009).

> Terrorist: He is not wearing glasses. Hey, … where are your glasses?
>
> Handler: … Is he bald from the front?
>
> Terrorist: Yes, he is bald from the front … he is fat and he says he has got blood pressure problems (Khetan 2009).

All these phone conversation evidences illustrate that the Mumbai terrorist group had a systematic mechanism of retaining the high level of situation awareness by monitoring live media and utilizing web search. They were collecting and analyzing up to date situation information from Pakistan, and the analyzed information was delivered wirelessly as an action command to the field attackers in Mumbai. Eventually, these situation assessment processes contributed to enhance the effectiveness of hand-held weapons terrorists used, and it resulted in calculated attack against civilians.

4 Content analysis of Mumbai twitter feed

This section discusses the issue of Web 2.0 social networking website from the perspective of information control and SA theory. As in the previous section, we posit that uncontrolled TV media and Twitter websites have potentially contributed to increase in terrorists' SA. To show the potential link of uncontrolled Twitter and terrorists' high level of SA, this section analyzes contents of Twitter postings.

Launched in July 2006, Twitter experienced around 900% growth during 2008 (Nusca 2009). Its rapid penetration speed seems to be related with 140 character based user interface which is compatible with the texting interface of mobile cellular phone. Especially, the compatibility of Twitter with text messaging interface of mobile phone lifted the constraints of wired connection to get connected with multiple people of social networking sites. This guess is supported by the report of PEW Research Center which states that, as of December 2008, more than 75% of Twitter users tend to search website wirelessly either on a wireless laptop, PDA, or mobile cellular phones (Lenhart and Fox 2009). Due to its mobile and rapid communication capabilities being equipped with a built-in digital camera, web browser, and digital camcorder, Twitter demonstrated its potential as emergency reporting systems in many natural disaster situations (Gabarain 2008; Mills et al. 2009; Wagner 2007). Subsequent to the successful reports of Twitter, US Federal Emergency Management Agency added Twitter to the national emergency response network (Tynan 2009). Now, a notion is being built surrounding Twitter that the cooperative relation between the public and the government is essential to conduct a successful operation during emergency situations.

The Mumbai Twitter page (http://www.twitter.com/Mumbai) that was used for data collection for this content analysis was voluntarily formed by online users and moderators to update and share the situational information of the Mumbai terrorist attacks. All postings that have been posted in the page were actual events that happened in Mumbai. Through this Twitter page, online users encouraged blood donation, posted contacts of Mumbai police help line, updated situational information of major Hotels and Nariman House which were under terrorist attack, signaled that s/he is in the site of terrorist attack, or broadcast their safety etc. Due to its real time postings by scene witnesses, news channels such as BBC, CBC, CNN, NPR, and Al-Jazeera etc cited messages from Mumbai Twitter page (Kievit 2008), and many users were followed and interviewed by worldwide mainstream media companies for their active postings. For example:

> "CNN (US) called me up—she said she saw my twitter and then flickr. Spoke to her for 10 mins. She might call me back again!"
>
> "#mumbai folks in south mumbai—if you're on skype video and can talk to a Toronto journalist, please contact @krisreyes"
>
> "journalists are looking for folks tweeting about #mumbai.please message @anlugonz from the BBC if you're interested in being interviewed"

The Twitter postings were more real and up-to-date than blogs and traditional news media. Some users added comments like "twitter rocks—I am getting accurate and better information than MSM like Times Now!" or "CNN has been playing catch up to twitter :)". Truly, Twitter played a significant role to relay situational information of the Mumbai terror attack to mainstream media around the world, and, at the same time, the live TV reports were linked back to Twitter.

However, as those live Twitter postings were made collectively and voluntarily in an uncontrolled ad hoc way, it included lots of sensitive situational information directly related to Indian government's operational activity. Consequently, it caused concerns from many Twitter users, because seemingly innocent postings and live coverage could potentially aid terrorists who were monitoring those media reports and online postings through satellite phones and other communication media. Furthermore, an online news source reported that "someone in India thinks Twitter offers a bigger risk than traditional blogging or even heritage media" (Riley 2008). Some exemplary postings of this genre include:

> "RT @celebcorps remember when tweeting details that it is CONFIRMED terrorists have satphone (*satellite phone*—authors added) access to net sources (1:50 AM Nov 27th, 2008 from Ubiquity)"

"Indian government has requested to stop tweeting live updates about Mumbai (8:08 AM Nov 27th, 2008 from web)"

"why is Times Now still revealing the strategy and positions of commandos @ Nariman House? #mumbai (3:58 AM Nov 28th, 2008 from twhirl)"

Our analysis of Mumbai Twitter data showed that concerns about uncontrolled collective Twitter postings were not groundless. To identify the Twitter postings that could have been beneficial for remote handlers in Pakistan to enhance their level of SA, we conducted a content analysis with posting data of the Mumbai Twitter page.

Content analysis is a research method that describes manifest content of communication in an quantitative, objective, and systematic way (Kishore et al. 2004–2005). This method is widely used in information systems research. Following the recommended steps (Krippendorff 1980; Meindl et al. 1985), we used SA theory framework to create a coding scheme. As the value of SA information is decided against an actor's goals, we used the three point political agenda of Mumbai terrorists as our coding scheme: anti-India, anti-Israel and anti-Jewish, and anti-US and anti-NATO (Raman 2009). If a Twitter posting contains information that could have been beneficial to increase SA of remote handlers in Pakistan such that they could either avoid Indian security forces' suppression activity or mount counter attack against civilian, then the Twitter posting was coded as '1'. Some exemplary postings that were coded as '1' are as follows:

"http://tinyurl.com/5wr2v6 helipad at the bottom right and Nariman house at the top left ... look at zoom level"[2] (6:13 PM Nov 27th, 2008 from web)

":)! RT@thej Friend: How come top ATS[3] cops got killed not other police men? Me: Dude it's not IT industry" (10:34 PM Nov 27th, 2008 from web)

"Retweeting @baxiabhishek: #mumbai Richard Stagg, British High Comisioner flew from New Delhi and is on the ground at Taj Hotel. Impressive." (10:56 PM Nov 26th, 2008 from twhirl)

Two masters' students in the US, majoring in management information systems were employed to separately code Twitter data. One was a student of a large Northeastern University, and other a student of a large Southeastern University. Both students had personal deep knowledge of the location (Mumbai) and its surroundings. Before coding, three phone conferences were instituted to discuss and understand the context and history of the Mumbai terror attack and the Mumbai Twitter page. It was ensured that both clearly understood the three point political agenda of the Mumbai terrorist group and the SA concept. The coding was made in two rounds. The first round was a pilot test to verify the level of mutual understanding of the research topic and coding scheme.

After the first round of content analysis, one author and the two coders had a phone conference with disagreed data. The author moderated disagreement between coders, refined the coding scheme, confirmed mutual understanding, and then worked on the second round coding of which result is represented as Table 1. The Kappa coefficient value was 0.965, which represents the extent to which the probability of agreed understanding between coders is higher than that can be obtained by chance (Krippendorff 1980). Our Kappa value confirms that the inter-coder reliability is reliable.

In Table 1, the first columns indicates three political agendas of Mumbai terrorist group which was identified by Raman (2009). The second column presents exemplary Twitter posts which can be beneficial for Mumbai terrorist group in enhancing their SA to accomplish their specific political goal (in the first column). The third and last columns show number and percentage of Twitter posts belonging to each political goal of the Mumbai terrorists. That is, out of total 934 Mumbai Twitter posts, 17.98 percent of posts contained situational information which can be helpful for Mumbai terrorist group to make an operational decision of achieving their Anti-India political agenda. Also, 11.34% and 4.6% of posts contained operationally sensitive information which may help terrorist group to make an operational decision of achieving their political goals of Anti-Israel/Anti-Jewish and Anti-US/Anti-Nato respectively.

5 Information control framework

Following the SA theory, the result in Table 1 shows that the situational information in the second column retains a complementary relationship with a specific political goal indicated in the first column. In other words, situational information in the second column alone does not have any signification or directional value for terrorist group's decision making until each situational information in the second column is processed through different political goals in the first column. Following the terminology of SA theory, the situational information (in the second column) remains at level one ("perception") in the SA chain. At this lowest level, the remote handler of the terrorist group simply "perceives" the situational information without comprehension of its informational value. However, when the situational information is processed by their specific political goals, a meaning begins to emerge with a particular directional value. This process belongs to level

[2] The URL is a link to Google map which indicates Nariman House under terrorist attack.
[3] ATS stands for Anti-Terror Squad

Table 1 Content analysis result of Mumbai twitter data

Political Goal	Situational Information (Sample Twitter Postings)	# of situational info / # of total posting	% of situational info
Anti-India	"#mumbai - avoid stepping out tomorrow to avoid chaos on roads. Govt offices will remain open."	168/934	17.98%
	"#mumbai - interviewing a Korean who's wife is still stuck in the Old wing. They were taken to the rooftop. He hasn't talked to her yet."		
	"Live gunfire outside Bombay hospital near metro cinema acc. to NDTV. Fear that terrorists will enter the hospital. Mumbai blasts"		
Anti-Israel and Anti-Jewish	"RT @robpas - Stratfor via IBN is reporting that there are Jewish and Israeli hostages at the Chabad House in Mumbai, India #mumbai."	106/934	11.34%
	"mumbai Authorities attack Nariman House with commandos and helicopter"		
	"#Mumbai DG of NSG on Times Now. Nariman House - 5 hostages dead bt 1,2,4 floor so far. 3rd floor is still not clear."		
Anti-US and Anti-NATO	"#mumbai Times Now quotes British high commission saying 7 British citizens injured in attacks."	43/934	4.6%
	"mumbai Official death toll now 101 including several Australians, one Japanese national"		
	"Retweeting @baxiabhishek: #Mumbai Richard Stagg, British High Commissioner flew from New Delhi and is		
	"Retweeting @baxiabhishek: #Mumbai Richard Stagg, British High Commissioner flew from New Delhi and is on the ground at Taj Hotel. Impressive"		

two of SA chain in which the remote handler of field terrorists understand the value of the situational information in conjunction with their political goal to achieve. Once the remote handler understands the informational value, they "project" the comprehended meaning of the situational information to the future to predict the future state or event after the action, which belongs to level three in the SA chain. For example, when terrorists observe situational information that a Korean wife "is still stuck in the Old wing," if they anticipate that killing her can prevent Koreans from investing capital in India, then they may kill her to complete their Anti-India political goal.

In conjunction with SA theory, Table 1 provides a clue to conceptualize the information control framework to deter or prevent decision-making process of terrorist groups. As SA theory posits and our analysis of terrorists' phone conversation shows, the value of situational information is interpreted and determined by their political goals. Therefore, their political goals can be seen as the interpretive scheme to process situational information. This interpretive scheme is represented as a vertical axis in Fig. 2, and, in case of Mumbai terror, it was composed of three prolonged political agenda: anti-India, anti-Jewish, and anti-NATO.

Using this interpretive scheme, terrorists process situational information following three staged cognitive process of "perception," "comprehension," and "projection," which is represented on the horizontal axis. Looking at our suggested information control framework in Fig. 2, we can see that terrorist's "perception" is triggered by situational information which is obtained through monitoring of live TV or websites. At this stage (Level 1), as the given situational information is not filtered through interpretive scheme (three political goals), the information itself does not contain any meaningful value which can lead to terrorist's decision making.

However, when the situational information passes through interpretive scheme (three political agenda) at level two ("comprehension"), the information is weighted with value for terrorist group to make calculated decision for their action. Once the value of situational information is determined by interpretive scheme, terrorists can project virtual scenario (Level 3 "projection") to predict the

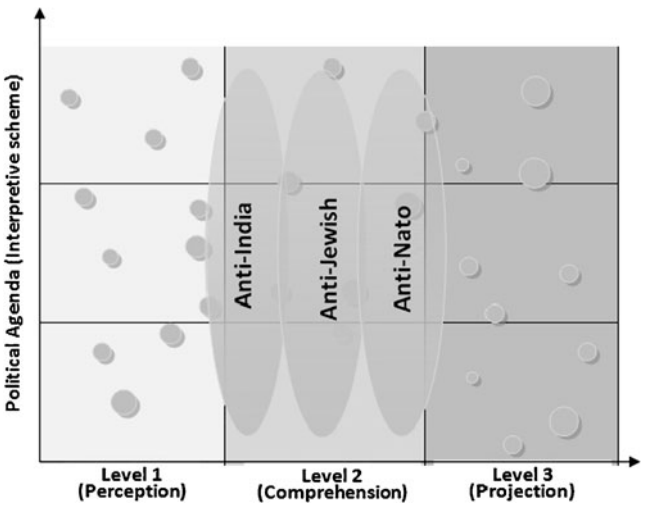

Fig. 2 Information control framework

outcome of their proposed action. Through this situation assessment process, if terrorists anticipate that their action can contribute to accomplish their political goals, then they will take their terrorist action.

Three staged situation assessment process of terrorist group (horizontal axes in Fig. 2) shows that, while the first stage ("perception") of the situation assessment is externally triggered through situational information which is posted by Tweeter users, the second stage ("comprehension") of situation assessment involves terrorists' cognitive (or interpretative) process upon the given situational information. That is, while the "perception" is triggered by external causes (situational information tweeted by Twitter users), the "comprehension" already involves terrorist's cognitive (interpretative) process, which pertains to terrorists' 'internal' attribute. Therefore, theoretically speaking, the information control measure to prevent terrorists' decision-making process must take place before the second stage ("comprehension") of situation assessment process by using terrorists' political goals as interpretative scheme (vertical axes in Fig. 2) to identify deleterious situational information. In other word, the vertical axes denotes the interpretative scheme which is required for security operation teams to identify deleterious information and make citizens aware which information is harmful or helpful for security operation with all possible communication channels such hyperlink, blog, RSS, email, text message, live TV and Retweet etc. Ideally, this step needs to be initiated before it reaches the second stage ("comprehension") of terrorist's situation assessment process.

Given Fig. 2, it is essential for government or anti-terrorism operation team to understand that information control strategy needs to be derived from thorough understanding of terrorist groups' political goals. Because terrorists' political goals function as interpretative filters to process situational information, understanding of adversaries' political goals may reduce costs for security operation teams to monitor and decide which tweets need to be controlled. Therefore, we suggest that the first step of information control in the context of participatory social reporting and terrorism is to analyze and understand the political agenda of terrorist groups.

When it comes to information control measures regarding participatory social media in the terrorism context, to the best of our knowledge, there are no references to refer to. This implies that the collective social reporting is not only a relatively new and rapidly growing phenomenon, but the Mumbai terrorist attack is the first incident which exposed the vulnerability of social reporting. However, to derive information control measures in the context of social reporting and terrorism, we can learn some lessons from the failure of media control during the wars such as Vietnam War (1959–1975), Faulklands War (1982), Grenada War (1983), Panama War (1989), Afghanistan War (2001 to present), and Iraq War (2003 to present) (Moore 2009; Hallin 1993). The war and media control literature highlight that modern wars require public support from both national and international levels to conduct successful operations.

In light of public support in anti-terrorism operations, as Weimann (2004) points out, "the use of advanced techniques" to control information—e.g. techniques "to monitor, search, track, and analyze communications"—"carries inherent dangers", as it can not only undermine public accountability and freedom of speech but lead to the loss of the public support. With this note of caution, we suggest an information control strategy. First, information control measure needs to be implemented in a way to encourage public accountability, and, at the same time, guarantee freedom of speech. Second, during terrorist attacks, government or security forces should monitor social reporting media such as Twitter and actively be involved in the social reporting process. That is, government and security forces need to make citizens aware what is harmful or desired information for security operation with credentials and authoritative voices by actively using such communication channels as hyperlink, blog, RSS, email, text message, live TV and Retweet etc.

We believe that the strength of our information control framework is that it is derived from detailed content analysis of real data including terrorists' actual phone conversation. That is, the suggested information control framework (Fig. 2) does not stand on artificial assumptions, but it reflects terrorists' decision-making process in real terrorist incident. Therefore, it is expected that the suggested information control framework can be enriched and refined by future researchers.

6 Conclusion

Our qualitative analysis of terrorist's phone conversation supports the validity of SA theory in analyzing terrorists' decision-making process. Through this analysis, we found that Mumbai terrorists actively monitored live media and used web search engines as a means to enhance their level of SA. Also, our close reading of Mumbai Twitter data found that the Twitter site played a significant role in relaying situational information to the mainstream media, which was monitored by Mumbai terrorists. Therefore, we conclude that the Mumbai Twitter page indirectly contributed to enhancing the SA level of Mumbai terrorists, although we cannot exclude the possibility of its direct contribution as well. Our quantitative content analysis of Mumbai Twitter data found that many Twitter posts (see above Table 1) could potentially have contributed to

enhancing terrorists' SA level by exposing operationally sensitive information without any information control. Based on these findings and following SA theory, we presented the information control framework, and argued that understanding terrorist groups' political goals is essential for successful information control. Also, one feasible information control measure was suggested.

Contributions of our research are as follows. Empirically, we identified how terrorists obtain and adversely use situational information, which is reported by networked citizens. Also, by interpreting phone conversation of terrorist group members through the lens of SA, we identified comprehensive process of their decision making in the extreme and uncertain condition of terrorist attack. Given that "the key to success in conflict is to operate within the opponent's decision cycle" (Taipale 2005), it is expected that identified terrorist group's decision-making process can serve as guidance for future research on terrorism and information control, especially in the context of wide spread Web 2.0 based social media.

As our description of terrorist's decision-making process was derived from the analysis of their actual phone conversation, we trust that this study sets the foundation for future researchers to investigate information control measures for social media in the terrorism context. It is worthy of mentioning that, to our knowledge, this research is the first report, which investigates the relationship between Web 2.0 based social media and terrorism with real case of the Mumbai terrorist attacks. Given that the Mumbai terrorist attack was the first incident in which participatory social media played significant role in spreading operationally sensitive information, we hope that the proposed information control framework can trigger further research to explicate the best information control mechanism in social reporting and terrorism context.

Our research has practical implications for national security policy makers, anti-terrorism security forces, and Web 2.0 based emergency reporting system designers in the terrorism context. They need to know that the Mumbai terrorist groups maintained a systematic mechanism of obtaining and maintaining high level of SA. Therefore, the best efforts needs to be made to find ways to deter or prevent terrorist groups from sustaining high level of SA either through information control policy, Twitter posting monitoring, or system design. Especially, given that the terrorists' decision making process is mainly driven by their political agenda, ongoing analysis of terrorist's political agenda will provide policy makers, anti-terrorism security forces, and systems designers with clues to build a strategic framework for information control. That is, they can develop information control policy or mechanism by employing the terrorist group's political agenda as interpretive scheme to decide which postings need to be controlled or not.

Acknowledgements This research has been supported by NSF under grant 0926371 and IIS-0926376 and 0929775. The usual disclaimer applies. We thank Shruti Jain and Himanshu Maheshwari, for help with the content analysis.

References

Anderson, A. (2003). Risk, terrorism, and the internet. *Knowledge, Technology, & Policy, 16*(2), 24–33.

Ariely, G. (2008). Chapter II: Knowledge mangement, terrorism, and cyber terrorism. In L. J. Janczewsk & A. M. Colarik (Eds.), *Cyber warfare and cyber terrorism* (pp. 7–25). New York: Yurchak Printing Inc.

Denning, D. E. (2009). Chapter 10: Terror's Web: How the Internet is Transforming Terrorism. In Y. Jewkes & M. Year (Eds.), *Handbook on Internet Crime.*Willan Publishing.

Endsley, M. R. (1995a). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), 32–64.

Endsley, M. R. (1995b). Measurement of situation awareness in dynamic systems. *Human Factors, 37*(1), 65–84.

Gabarain, C. (2008). Twitter and the Sichuan earthquake: proving its value?. http://eapblog.worldbank.org/content/twitter-and-the-sichuan-earthquake-proving-its-value (Accessed Nov. 15th, 2009).

Gartner (2010). Gartner Reveals Five Social Software Predictions for 2010 and Beyond, http://www.gartner.com/it/page.jsp?id=1293114 (Accessed June 6th, 2010). http://www.contentious.com/2008/11/27/tracking-a-rumor-indian-government-twitter-and-common-sens/ (Accessed June 6th, 2010).

Haeni, R. E. (1997). Information Warfare—an Introduction. The George Washington University Cyberspace Policy Institute, January, pp. 1–16.

Hallin, D. (1993). The uncensored war. *Peace Review, 51*(1), 51–57.

Hutchinson, W. (2006). Information warfare and deception. *Informing Science, 9*, 213–223.

Indian Ministry of External Affairs. (2009). "Mumbai Terror Attacks - Dossier of Evidence," http://www.hindu.com/nic/dossier.htm (Accessed June 4th, 2010).

Khetan, A. (2009). 60 dark hours at Hotel Taj. In H. Baweja (Ed.), *26/11 Mumbai attacked* (pp. 46–83). New Delhi: Roli Books.

Kievit, R. (2008). "Twitter messages feed major news channels," http://static.rnw.nl/migratie/www.radionetherlands.nl/features/media/081128-twitter-redirected (Accessed Nov. 9th, 2009).

Kishore, R., Agrawal, M., & Rao, H. R. (2004–2005). Determinants of sourcing during technology growth and maturity: an empirical study of e-commerce sourcing. *Journal of Management Information Systems, 21*(3), 47–82.

Krippendorff, K. (1980). *Content analysis: An introduction to its methodology.* CA: Sage.

Lee, W. E. (2002). Security 'review' and the first amendment. *Harvard Journal of Law & Public Policy, 25*(2), 743–763.

Lenhart, A., & Fox, S. (2009). Pew internet project data memo regarding Twitter and status updating. Pew/Internet.

McAfee, A. P. (2006). Enterprise 2.0: The dawn of emergent collaboration. *MIT Sloan Management*, Spring, pp. 20–28.

Meindl, J. R., Ehrlich, S. B., & Dukerich, J. M. (1985). The romance of leadership. *Administrative Science Quarterly, 30*(1), 78–102.

Mills, A., Chen, R., Lee, J., & Rao, H. R. (2009). Web 2.0 emergency applications: how useful can Twitter be. *Journal of Information Privacy and Security, 5*(3), 3–26.

Moore, D. W. (2009). Twenty-First Century Embedded Journalists: Lawful Target?. In A. M. Tulud, A. B. Ching & C. J. Strong (Eds.), *The Armay Lawyer* (pp. 1–32) Department of Army.

Nusca, A. (2009). "Twitter's active users grow 900% in one year," http://blogs.zdnet.com/BTL/?p=12919 (Accessed Nov. 10th, 2009).

Qin, J., Zhou, Y., Reid, E., Lai, G., & Chen, H. (2007). Analyzing terror campaigns on the internet: technical sophistication, content richness, and web interactivity. *International Journal of Human Computer Studies, 65*, 71–84.

Raman, B. (2009). "Mumbai terrorist attack - some aspects," http://globalpoliticsonline.com/wped/2009/01/17/mumbai-terrorist-attack-some-aspects/ (Accessed Nov. 15th, 2009).

Riley, D. (2008). "Report: Indian government trying to blck Twitter as terrorists may be reading it," http://www.inquisitr.com/9863/report-indian-government-trying-to-block-twitter-as-terrorists-may-be-reading-it/ (Accessed Nov. 9th, 2009).

Shachtman, N. (2008). "Spy Fears: Twitter Terrorists, Cell Phone Jihadists," http://www.wired.com/dangerroom/2008/10/terrorist-cell/ (Accessed June 4th, 2010).

Siegler, M. G. (2008). "Osama bin Twitter: Terrorists hone the micro-message," http://social.venturebeat.com/2008/10/26/osama-bin-twitter-terrorists-hone-the-micro-message/ (Accessed June 4th, 2010).

Strater, L. D., Endsley, M. R., Pleban, R. J., & Matthews, M. D. (2001). "Measures of platoon leader situation awareness in virtual decision-making exercise," US Army Research Institute for the Behavioral and Social Sciences.

Taipale, K. A. (2005). "Destabilizing Terrorist Networks: Disrupting and Manipulating Information Flows in the Global War on Terrorism," Yale ISP 2005 Global Flow of Information, Draft.

Tsfati, Y., & Weimann, G. (2002). www.terrorism.com: terror on the Internet. *Studies in Conflict & Terrorism, 25*, 317–332.

Tynan, D. (2009). "Twitter added to federal emergency response network," http://www.infoworld.com/d/adventures-in-it/twitter-added-federal-emergency-response-network-719 (Accessed Nov. 14th, 2009).

Wagner, M. (2007). "Google Maps and Twitter are essential information resource for California fires," www.informationweek.com/blog/main/archives/2007/10/google_maps_and.html (Accessed Nov. 14th, 2009).

Weimann, G. (2004). "www.terror.net: How Modern Terrorism Uses the Internet," Special Report, United States Institute of Peace (116), pp.1–12.

Onook Oh is a doctoral student of the Department of Management Science and Systems at State University of New York at Buffalo. He received his bachelor's degree of English literature at the Hallym University, and his MA at Seoul National University, Korea. Also, he received his MS degree of management science and systems at the State University of New York at Buffalo. Prior to joining the doctoral program he worked as a network system administrator, web programmer, and database developer. His current research interests are information ethics and collective intelligence.

Manish Agrawal is an Associate Professor in the Department of Information Systems and Decision Sciences of the College of Business Administration at the University of South Florida in Tampa, Florida. Dr. Agrawal teaches classes on Web applications development, information security and Computer Networks at both the graduate and undergraduate levels. His current research interests include Information security, Software quality and the development of application-specific Agent-based systems. His articles have appeared in jounals including Management Science, INFORMS Journal on Computing, IEEE Transactions on Software Engineering, ACM Transactions on Information Technology, Communications of the ACM and the Journal of Management Information Systems. He completed his PhD at SUNY Buffalo. Dr. Agrawal is a member of AIS and INFORMS.

H. Raghav Rao is a professor in the Department of Management Science and Systems of the School of Business at the State University of New York at Buffalo. Dr. Rao graduated from Krannert Graduate School of Management at Purdue University. His interests are in the areas of management information systems, decision support systems, e-business, emergency response management systems and information assurance. He has chaired sessions at international conferences and presented numerous papers. He also has co-edited four books of which one is on Information Assurance in Financial Services. He has authored or co-authored more than 150 technical papers, of which more than 100 are published in archival journals. His work has received best paper and best paper runner up awards at AMCIS and ICIS. Dr. Rao has received funding for his research from the National Science Foundation, the Department of Defense and the Canadian Embassy and he has received the University's prestigious Teaching Fellowship. He has also received the Fulbright fellowship in 2004. He is a co-editor of a special issue of The Annals of Operations Research, the Communications of ACM, associate editor of Decision Support Systems, Information Systems Research and IEEE Transactions in Systems, Man and Cybernetics. Dr. Rao also has a courtesy appointment with Computer Science and Engineering as adjunct Professor.