Journal of
Mass Communication & Journalism

Narula and Jindal, J Mass Communicat Journalism 2015, 5:2
DOI: 10.4172/2165-7912.1000246

Review Article Open Access

Social Media, Indian Youth and Cyber Terrorism Awareness: A Comparative Analysis

Narula S[1]* and Jindal N[2]

[1]HOI Amity School of Communication, Amity University, Madhya Pradesh- 474020, India

[2]Assistant Professor, Amity School of Communication, Amity University , Madhya Pradesh- 474020, India

Abstract

Cyber Terrorism is one of the most ignored and under estimated activities in India. Indian Youth which is the third highest number of Internet and social media users after China and the U.S. with an estimated over 381 million mobile phone subscriptions with Internet connectivity. Cyber Terrorism has now become a gruesome activity, it leads to killing someone financially and India is becoming its latest victim. Everyday various newspapers are filled with the stories of cybercrimes. It is not a future threat or a prospective threat; it is an ongoing, current threat.

With increasing dependence on cyber space and the Internet, vulnerability to aggressors — whether it is terrorists, criminals or hostile countries, is also increasing. In this study, the habits of teenagers all around India shows the compulsive type of behaviour of text messages but very less knowledge and awareness about the threat of cyber terrorism. These facts not only outline in clear terms the immense popularity of the internet and the use of social media but are also indicative of the fact that Indian youth is very less concerned about the threat of cyber terrorism.

Keywords: Cyber Terrorism; Social Media; Terrorists

Rationale

The present study tries to comprehend the concept and understanding of Cyber Terrorism as a phenomenon. The study will look into the following factors, in order for a better understanding of the concept of cyber terrorism.

- The profile of the cyber media user
- Users' understanding of the term 'Cyber Terrorism'
- Users' knowledge of fundamental security acts
- Users' perspective on India's stature in handling the plague of cyber terrorism.

Introduction

Social media has become such a pivotal part of our lives that we find it almost impossible to survive without it. The virtual world has replaced the real world to a great degree. What we spoke in get-togethers and drawing room discussions, is spoken via social media now. General observations tell us that this has risen to the extent that people sitting in a group would be less likely to talk to each other and more indulged in conversations on social media.

The time and amount of energy Indian youth spends on social media, clarifies the significance of the same in their lives. However, they are not sensitized about social media. It is very significant that the users know how to handle sharing of content and information in the virtual space. The youth finds social media attractive and addictive, and a very good means of conversing with their friends, family or strangers. But if they realize the severity of sharing sensitive information on social media, remains a big question [1].

Social media has undoubtedly, revolutionized our lives in a manner we would have never thought, a decade ago. Information at finger-tips is an understatement. In addition, we use social media on our mobile phones, which has further simplified information sharing and gathering. Majority of smart phone users (operating systems- android, iPhone, Windows), utilize applications to ease everything from using social network sites, surfing, checking emails, booking movie tickets, or train tickets and the like. Nevertheless, what they little realize is that sharing of sensitive information like Debit Card and Credit Card passwords and similar other PINs, can reveal all of this information to servers, and there is likelihood that your personal accounts, if not hacked, are tempered or compromised with.

Cyber crimes are increasing by the day and new media users are oblivious of the consequences. The users make use of internet very callously, thinking that their internet movements aren't noticed anywhere and cyber terrorists benefit from this. When youngsters share sensitive information on social media, all these facts, are sometimes unintentionally not considered. The ICT revolution has given rise to 'cyber terrorism', which has become a gruesome threat to combat because of its intangible nature. It becomes a technical difficulty for the common man to understand the use or misuse of cyber space, which can lead to cyber threats. Besides, insecure internet connections can also divulge your personal information to outside servers.

Youngsters need to be sensitized towards the appropriate use of virtual space, about the sharing of any kind of content, information, photographs, and links on the social media. Awareness about appropriate use of social media is very essential, to curb any form of cyber terrorism. For this, it is also important that one is adept with

***Corresponding author:** Narula S, Ph.D, HOI Amity School of Communication, Amity University, Madhya Pradesh- 474020, India, Tel:9560452625; E-mail: suminarula@gmail.com

Received January 26, 2015; **Accepted** February 18, 2015; **Published** February 28, 2015

Citation: Narula S, Jindal N (2015) Social Media, Indian Youth and Cyber Terrorism Awareness: A Comparative Analysis. J Mass Communicat Journalism 5: 246. doi:10.4172/2165-7912.1000246

Copyright: © 2015 Narula S, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

regard to technology as well, to keep oneself safe from any sort of cyber attacks [2].

Cyber terrorism defined

Cyber terrorism can be defined as electronic attacks from cyberspace from both the internal and external networks, particularly from the Internet that emanate from various terrorist sources with different set of motivations and are directed at a particular target (Axelrod, C. Warren. "Security Against Cyber Terrorism). Cyber terrorism pertains to damaging, misusing, or compromising with a nation's high-profile works or ventures or its security. However, they are not restricted to it, and hackers can also malign reputations of smaller organisations or even individuals, leaving a major psychological impact.

A report published by PCWorld.com online magazine in 2001 stated that the Federal Bureau of Investigation (FBI) and the System Administration, Networking, and Security Institute (SANS) had released a list of the 20 top vulnerabilities of Internet-connected systems and urged organizations to close the dangerous holes in order to avoid major cyber terrorism attacks. According to Allan Paller who is the SANS Institute Director in the article, "The Internet is simply not ready because of these vulnerabilities; we're not ready to withstand a major attack" [3].

According to Computer Crime Research Centre (CCRC), "there is a lot of misinterpretation in the definition cyber-terrorism, the word consisting of familiar 'cyber' and less familiar 'terrorism'. While 'cyber' is anything related to our tool of trade, terrorism by nature is difficult to define. The ambiguity in the definition brings indistinctness in action, as D. Denning pointed in her work Activism, Hacktivism and Cyberterrorism, 'an e-mail bomb may be considered hacktivism by some and cyber-terrorism by others (Krasavin, Serge). Cyber terrorism can thus be understood as unauthorized internet activity or attack on computer networks that may threaten the private internet space of an individual, organisation, entity or a nation.

Cyber terrorists

The term 'cyber terrorists' cannot be related to the term 'terrorists' per se. However, cyber terrorist can be an individual or people who aim to damage their 'target's' reputation, and put them under mental trauma. The targets are primarily computer networks of either organisations or individuals. Cyber terrorists are also known by the term 'hackers', who are most of the times amateurs, and are by far the biggest threat on the Internet at the current time. They are responsible for about 90% of all hacking activities. 9.9% are potential professional hackers for hire (corporate spies), and a mere 0.1% are world-class cyber criminals [4].

Review of Literature

The studies under review suggest that with the use of media, cyber terrorism operation can be undertaken from miles away. Cyber terrorism attacks have an equal capacity of inflicting serious damage. When cyber terrorists attack, they attack on infrastructures, monetary systems, power grids and other sensitive information [5].

Another study with a rather contradictory view states that Electronic Disturbance Theater (EDT) is known to have constantly conducting Web sit-ins since December 1997 against varied sites in support of the Mexican Zapatistas. The findings of this study reveal that at a stipulated time thousands of protestors point their browsers to a target site using the software and this leads to a flooding of download requests at the target. However, this is believed to have been used by activists more than by hackers or terrorists [6].

A 2000 Japanese investigation found out that the government was making use of software that was found to have been responsible for the Sarin gas attack on the Tokyo subway station in 1995. As good as 10 Japanese government agencies came out in the findings to have been using as much as 100 types of malicious software programs [7]. Furthermore, programs developed by Aum Shirinkyo were suspended, with the threat of invasion of privacy, planting malicious content or code or crippling computer systems.

The recent loss of control of the New York Times, Twitter and the Huffington Post of some of their websites (2013) "after hackers supporting the Syrian government breached the Australian Internet company that manages many major site addresses", is a significant example in the case studies of cyber terrorism. The target of the Syrian Electronic Army, a hacker group has been organisations that it considers hostile to the Syrian President Bashar al-Assad [8].

Research Design

The method used for the study is a survey, filled in by selected candidates, the answers of which were later analysed. A sample size of 150 candidates was taken for this survey, out of which 75 were students of legal studies and the remaining half was from varied academic disciplines. The purpose was to get a specialised and a generalised view on various aspects of cyber terrorism. The study aimed at youngsters' understanding of the concept of cyber terrorism, and they related it to media.

It was also an aim to find out as to what was the extent to which cyber terrorism was associated with media. For this, a strategically designed questionnaire was given to the survey participants to gather qualitative data and their responses were later analysed via inferential statistics (a method wherein we try to infer from the sample data what the population might think of the topic or issue under discussion).

Data Analysis and Presentation

The study conducted to observe how people understand the concept of cyber terrorism and how they relate it to media. The study shows that out of a 150 respondents, 73.33% respondents used the internet, while 20% admitted to not using it, and another 6.66% didn't agree to either of the choices.

Out of the total, 46.66% stated that they understood the concept of cyber terrorism, 40% didn't understand the notion and 13.33% had some bit of knowledge about it. This shows that the youth is merely reasonably updated about the latest trends with regard to social media threats but could use some more knowledge. Furthermore, 36.66% of the respondents claimed that their accounts have been hacked, 50% said that their accounts have never been hacked, and 13.33% said that they were not sure about the same. It can also be added as an observation that out of the 50% that says their accounts have never been hacked; a possibility of their accounts having been compromised at a certain level sure exists, out of their knowledge, which could perhaps add on to the category of being unsure about the same.

We further understand that a majority uses online shopping services and this amounts to a 60% while 13.33% does not shop online, and 26.66% uses the online shopping facilities at times. While a majority uses internet facilities to shop online, there wasn't much debate about this number knowing cyber laws and security measures *to-the-t*, with regard to shopping online. Concerning cyber security, about 54% considered cyber terrorism a threat, while 13.33% couldn't

make up their mind for the same, and 33.33% observed that it wasn't of a very serious nature. Further to this, 10% couldn't comment when asked if India was ready to tackle the threat of cyber terrorism, 43.33% believed that India could fight the problem and 46.66% said that India couldn't deal with it.

Furthermore, 13.33% of respondents knew about the India Information Act, however limited. Another 46.66% did not know about it, and 40% had good workable knowledge regarding the same. We also come to know that 43.33% of the candidates were aware of the penalties levied in the Indian constitution, while 46.66% was caught unawares and 10% wasn't sure if their knowledge on this topic was sufficient, in general or to put up a decent conversation.

Further next, was the issue of cyber terrorism being covered by Indian media, wherein 43.33% responded negatively, and 46.66% was in favour of it and 10% was unsure. With regard to cyber laws, 60% believed that freedom of media shouldn't be taken back, rather cannot be. A meager 7% couldn't comment on the same and 33% said that freedom of media should be taken back.

Presentation of analysed data

The tabular data is a presentation of candidates' responses of the questionnaire (Tables 1a-1i) (Figure 1).

S. No.	Topic	Percentage
1	Use of cyber media	73.33%
2	Non-usage of cyber media	20%
3	Can't say	6.66%

Table 1a: Do you use Cyber media/Internet?

S. No.	Topic	Percentage
1	Understanding of cyber media	46.66%
2	Non-understanding of cyber media	40%
3	Somewhat	13.33%

Table 1b: Do you understand Cyber Terrorism?

S. No.	Topic	Percentage
1	Email/Bank account hacked	36.66%
2	Email/Bank account not compromised	50%
3	Not sure	13.33%

Table 1c: Has your email/bank account ever been hacked/compromised with?

S. No.	Topic	Percentage
1	Online shopping	60%
2	No shopping online	13.33%
3	Sometimes	26.66%

Table 1d: Do you use online shopping services?

S. No.	Topic	Percentage
1	Cyber terrorism as a threat	53.33%
2	Not very serious	33.33%
3	Can't say	13.33%

Table 1e: How do you rate Cyber terrorism?

S. No.	Topic	Percentage
1	Countering cyber terrorism- Yes	43.33%
2	Countering cyber terrorism- No	46.66%
3	Can't say	10%

Table 1f: Is India ready against any cyber terrorism threat?

S. No.	Topic	Percentage
1	Good knowledge of cyber laws	40%
2	No knowledge of cyber laws	46.66%
3	Reasonable knowledge of cyber laws	13.33%

Table 1g: Do you know about India Information Act 2000?

S. No.	Topic	Percentage
1	Indian media's coverage of cyber terrorism is good	46.66%
2	Indian media's coverage of cyber terrorism is below mark	43.33%
3	Can't say	10%

Table 1h: Is Indian Media covering news of Cyber Terrorism?

S. No.	Topic	Percentage
1	Should freedom of media be taken back- Yes	33%
2	Should freedom of media be taken back- No	60%
3	Can't say	7%

Table 1i: Should Freedom of media be taken back?

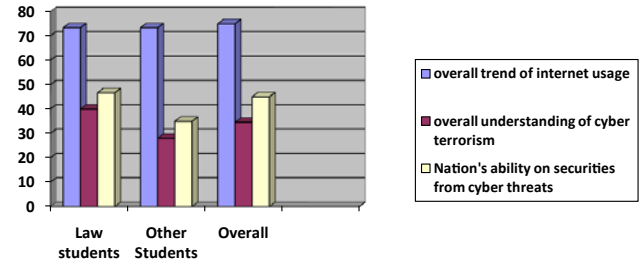

Figure 1: The graph shows an overall perspective on students' (Law and others) understanding of the concepts of cyber media and cyber terrorism, and their viewpoints on nation's ability in tackling cyber threats.

Conclusion

The study reveals that people relate media and cyber terrorism and understand that with the rise of the usage of media in general and the internet in particular, cyber terrorism has escalated as a phenomenon too. Nonetheless, youngsters utilising the internet facilities are not much aware of cyber laws, and the ways they can be safe from hackers and cyber terrorists. The internet usage is increasing by the day, and the number of people shopping online, sharing content, photographs, videos and links is rising too.

During these activities, many a time not much attention is paid on the fact that sharing sensitive information online (bank account PINs, social security codes, personal information like photographs etc.) can prove detrimental. Hackers and cyber terrorists misusing such information can lead to not only monetary loss (in case of bank account details), but loss of important information and dignity (in case of personal information and photographs). Such information is picked up from servers, and compromised with to damage a person's reputation, or an on organisation's business leading to financial strain.

The response also revealed a need of better technology and cyber security measures to deal with the plague of cyber terrorism. A majority agreed that we lacked in cyber security measures and the issue is not addressed very appropriately in the Indian media. There was more attention required to address the problem of cyber terrorism overall.

There is another case in view, which is different perspectives on cyber terrorism as a phenomenon. The cases here are of law students and students from various other academic disciplines. As far as usage of

internet or cyber media is concerned, it is understood that there really is no difference or variation depending upon the academic discipline, and that students from the law department and rest other departments were at par. The difference was found in the understanding of cyber terrorism wherein the participants studying law seemed to have a better score of knowledge on the same. Furthermore, with regard to cyber securities, it was understood that participants of the law department held the view that the nation's ability of dealing with cyber terrorism was fairly good. However, this percentage was lesser in the responses of students from other academic disciplines.

References

1. Mitnick KD, Simon WL (2002) Controlling the Human Element of Security: The Art of Deception. Kineticstomp, Swift.
2. Ayers C (2009) The Worst is Yet to Come" Futurist.
3. Thibodeau P (2001) Internet Vulnerabilities to Cyberterrorism Exposed. Computer World.
4. Sproles J, Byars W (1998)Statistics on Cyber-terrorism.
5. Matusitz J (2005) Cyberterrorism. American Foreign Policy Interests 2: 137-147.
6. Perlroth N, Sanger DE (2013) Corporate Cyberattacks, possibly State-backed, Now Seek to Destroy Data. The New York Times.
7. Maryann CL (2001) Public Private Partnerships and Global Problems:Y2K and Cybecrime. Paper Presented at the International Studies Association, Hong Kong.
8. http://archive.thedailystar.net/beta2/news/new-york-times-twitter-hacked-by-syrian-group/