International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Security Threats in Indian Cyberspace by Social Media and Cyberhoaxes

Dr. Ashok Koujalagi, Thrupti N S, Karuna Kurbet
Asst. Professor & Postdoctoral Researcher
P.G Department of Computer Science, Basaveshwar Science College, Bagalkot, Karnataka, India

ABSTRACT

This study examines the proliferation of hoaxes and hate speech through websites and social media in India. Such provocative content utilizes sectarian issues to attack its creators' political opponents. This study finds that hate has been politicized and hoaxes have been commodified, both for economic and political interests, in Indian cyberspace. There has been a transformation from freedom of speech to freedom to hate, particularly on social media networks. This proliferation of hoaxes, as a means of furthering specific political interests, may potentially threaten national security and stability. To overcome the threat posed by cyberhoaxes, the state, industry, and society must take an active role in protecting cyberspace.

Keywords: *Cyberhoax; Cyber Security; Freedom to Hate; Politics of Threat*

I. INTRODUCTION

Hoaxes and fake news have become increasingly common in India, particularly on the internet and social media. This was not the first time that hoaxes spread in India. For example, during the 2014 Indian Prime ministerial election deliberately disseminated provocative fake news and emphasized sectarian issues to attack political opponents. Similar cases have occurred in the United States, Germany, China, France, and Malaysia, where accurate news has been mixed with gossip and hate speech before being rapidly spread through social media.

The proliferation of hoaxes has been made possible through the widespread adoption of Facebook, Twitter, WhatsApp, Line, Google+, and other new media platforms, which have made the rapid dissemination of information possible through their high degrees of interactivity and interconnectivity. Hoaxes have spread uncontrolled through cyberspace, and some have had serious social implications. In response to hoaxes, people have been killed and national stability and security has been threatened. Most hoaxes have involved fake news about sensitive tribal, religious, and racial issues as well as hate speech directed towards those in power.

The cyberhoax phenomenon has become crucial in an Indian context, and as such requires serious attention, particularly given that half of Indians are active internet users

II. CYBERHOAXES IN INDIA

In India, the emergence of new media has invigorated civil society and empowerment movements, particularly following the fall of the New Order regime. Cyberspace has seemed to promise citizens the freedom of expression and active participation in political processes. At the same time, general elections, a common manifestation of the democratization process, have been faced with intense public distrust. Few citizens trust political parties or the commitment and performance of politicians. There has been considerable public disappointment in and resistance to political processes. In cyberspace, people have greater opportunity to voice criticism and resist those in power, something not possible under

authoritarian regimes. However, resulting excesses have become the basis for fake news and hate speech in India

III. THE PRODUCTION AND DISSEMINATION OF HOAXES IN INDIA

The Cyberhoaxes perpetrated by the five websites investigated in this researcher utilize a similar modus operandi. Desiring to criticize the government in power, the website administrators use cyberspace to voice their aspirations, holding that social media and microblogs do not offer them sufficient space to promote their interests. Visibility is a central aspect of public.

The desire for visibility and attention, not only from those being criticized but also from others, underlay administrators' decision to create websites where they began producing hoaxes. These websites lack clear information on their founders, and their "About Us" pages appear perfunctory or even deceptive. Information on these websites' organizational structures and addresses are often not included.

At their core, these hoax websites rely on the journalistic products of the mainstream media. In selecting specific issues, they observe mainstream media coverage. Issues with the potential for controversy and support the administrators' own interests (or can be used to attack their opponents) are identified and selected. The issues they select are modified by administrators using one or more of the techniques discussed below. First, facts may be exaggerated with fiction, particularly that which can be mobilized to promote tribal, religious, and racial tensions and hatred. Second, the substance of the story may remain unchanged, but be given a provocative and bombastic headline. Third, the main points of the coverage may be maintained, but presented in clear, direct, and provocative language. Fourth, the titles of photographs or illustrations may be changed to make them more provocative. Fifth, photographs or illustrations of incidents unrelated to that being covered may be used to suggest a connection and thereby provoke readers.

Aside from modifying coverage from the mainstream media, the administrators of these websites may also cover statements and opinions from politicians and commentators who share their vision. To do so, the administrators cultivate relations and friendships with such politicians and commentators, who are frequently opposed to existing government policy. Furthermore, these politicians and commentators are used as references or given space to voice their (anti-government) opinions on the websites.

The fake news and hate speech produced by these websites are not journalistic products that follow the accuracy and accountability standards of the profession. However, the website administrators do not care that their content violates journalistic principles.

IV. PRODUCTION OF UNCERTAINTY: POLITICAL SYMBOLISM AND MISINFORMATION

As economic and political commodities, hoaxes represent an exchange of deceptive and inflammatory symbols. the use of such symbols in a political context is an element of political symbolism The proliferation of symbols, including their use and misuse, is intended to manipulate political discourse and public opinion, According to Edelman, symbols have taken an increasingly important role in politics. Political influence and power is no longer based on material and objective facts, but the mobilization of symbols. For example, political symbolism is rampant in political campaigns. argue that political practices in the digital media ecosystem emphasize the exploiting of various symbols for mass mobilization and manipulation.

In the practice of hoaxing, linguistic symbols (both verbal and visual) are used to construct certain views of the issues discussed. identifies two different types of symbols used in political practice symbolism: referential symbols and condensation symbols. Referential systems are those related to objective elements of certain situations and objects. These symbols are frequently used to legitimize specific political views and guide the masses towards a specific and shared understanding of a situation or object, such as statistics or budgets. Meanwhile, condensational symbols are those that create certain emotions and subjective reactions to a situation or object. Such symbols are capable of shaping people's imagination of a desired world, one quite different from the real world. It is such condensational symbols that are mobilized by cyberhoaxes in Indonesia. Nonetheless, according to Edelman, both types of symbols can be used to manipulate public discourse and public opinion about certain issues. This is one-sided, intended to justify specific ideas and logics.

In cyberspace, political symbolism promotes specific simplified narratives and framings of certain situations and objects. The new media, which enables

the consumption of information (and distraction), contributes importantly to this symbolization process. This can be seen, for example, in the use of clickbait, in which symbols (images) in cyberspace serve are provided as "keys" to exploring issues and problems. Through clickbait, overly simplified logics are brought into the digital ecosystem. The (over)simplification of narratives is common in new media, and consequently very few media users seek detailed information or seriously investigate the events and processes reported. Spaces for discussion and reflection disappear as access is accelerated. Events and processes are framed as nothing but headlines.

V. COMBATTING AND PREVENTING CYBERHOAXES

The production and dissemination of cyberhoaxes and hate speech are part of the politics of threat and designed by certain actors to promote certain interests. Hoaxes, as with cyber threats in general, are not material, nor do they cause direct physical harm to humans. Nonetheless, they have serious social effects. In other words, the cyberhoaxes that have become increasingly widespread in India have the potential to threaten national stability.

To combat cyberhoaxes, three different parties must work together: the state, market, and civil society. They must collaborate to address various strategic issues that threaten cybersecurity (in particular), as well as national security and stability in general. In the context of national authority, specific legal products must be prepared to provide stricter judicative sanctions. To provide cybersecurity in India, particularly against cyberhoaxes, it is possible to apply this latter concept, for example by regulating domain ownership and setting fines for platform providers. Furthermore, it is important to increase the capacity of the State's cyber troops.

As such, the Indian government must act to change those regulations it has enacted. The Indian government must transform the regulations applicable to the media platforms used to make hoaxes go viral. Thus far, India has not provided for any fines for them, relying solely on blocking mechanisms—even though forcing platforms such as Facebook and Google to pay large fines if they fail to remove fake news, hate speech, and hoaxes may serve to limit their spread on social media.

CONCLUSION

The creation and dissemination of cyberhoaxes in India is a deliberate practice intended to promote certain motives and interests. It is perpetrated by actors who seek to spread deceit and hate in the digital ecosystem. The proliferation of hoaxes in cyberspace indicates a shift from freedom of speech (facilitated by new media platforms) into freedom to hate, which is used to attack those opposed to them. The websites in this study use similar production patterns. To draw public attention, they mobilize rumors and tribal, religious, and racial sentiments. To popularize their websites, hoaxers use social media and networks to spread fake news and hate speech. The proliferation of hoaxes and hate speech in cyberspace threaten national security and stability.

References

[1] Allcott, H. and Gentzkow, M., “Social Media and Fake News in the 2016 Election”, Journal of Economic Perspectives, Vol. 31, No. 2, pp. 211–236, 2017.

[2] Arnhart, L., “Murray Edelman, Political Symbolism, and the Incoherence of Political Science”, Political Science Reviewer, Vol. 15, No. 1, pp. 185–213, 1985.

[3] Bernstein, R. J., Hannah Arendt and the Jewish Question. Cambridge: Polity Pres, 1996.

[4] Cavelty, M.D., Cyber Security and Threat Politics: US Efforts to Secure the Information Age. London, New York: Routledge, 2008.

[5] Dahlgren, P., The Political Web: Media, Participation and Alternative Democracy. New York: Palgrave Macmillan, 2013.

[6] Edelman, M., The Politics of Misinformation. Cambridge: Cambridge University Press, 2013.

[7] Eriksson, J. and Giacomello, G., International Relations and Security in the Digital Age. London, New York: Routledge, 2007.

1) Lash, S. and Urry, J., Economies of Signs and Spaces. London, Thousand Oaks, New York: Sage, 1993.