Social Media Exploitation for Terrorism

RajKumar[1], Neha Singh[2], Arbaz[3]

[1]*B.Tech (CTIS), Teerthanker Mahaveer University, Moradabad*

[*] *Assistant Professor*
iNurture, Teerthanker Mahaveer University, Moradabad

[3]*B.Tech (CTIS), Teerthanker Mahaveer University, Moradabad*

[1]rajkumarmbd0455@gmail.com

[2]neha.s@inurture.co.in

[3]arbazahmed010101@gmail.com

Abstract— **With the evolution of technology, social media have emerged as a vibrant platform for dissemination of information to the masses. The easy accessibility of this platform has motivated the users to share their thoughts and perception and even inspire their surroundings for some social general cause. However this technology also has a flip side which is being exploited by the terrorist to distract and misguide the groups for their personal intentions. This paper will focus on how social media have been exploited by terrorist to hamper the society beliefs and create agitation among groups and communities. The aim of this study is to examine the terrorist activities propagated through social media.**

Keywords— **Cyber Terrorism, Social Media, Cyber Espionage, Cyber Warfare**

I. INTRODUCTION

Terrorism cannot be defined in words; in fact there is no universally accepted definition for it."Terrorism" can only be understood as “to use violence to make fear among the people to complete religious or political or ideological agenda”. When terrorism exploits the platform of electronic mass communication i.e., to use internet or technology of web to make a terror attacks, it is termed as cyber terrorism. Keith Lourdeau define terrorism as "Cyber terrorism is a criminal act perpetrated by the use of computers and telecommunication capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda."[1]

Cyber terrorism is the combination of weapons and technology, or it can be said that today some people are using information technology as the weapon of terrorism. Almost every people are connected to internet now so it is the easiest way to harm a large number of people in a very small pace. The serious consequences that they hold are causing destruction of person or property and building fear among the people.

Now a days, the terrorist groups are focusing on social media for propagating their agenda. Because of easy accessibility of internet facility, masses are communicating their thoughts through these social media platforms. This paper offers a thorough and detailed review of exploitation of social media platforms by various terrorist groups.

II. CYBER TERRORISM

Terrorism has threatened humanity and destroyed world peace through ages. The fight to defeat terrorism has united the nations across the world on a common front. But with the passing of time controlling this evil phenomenon has become even more difficult, as now the perpetrators conduct their activities against democratic societies with much newer and modern weapons of war. One of the cheapest and easiest ways to generate fear in the society by a single actor is through Cyber-terrorism or cyber warfare.

Cyber Terrorism is assumed to be as one of the categories of cyber threats. Along with cyber terrorism the other threats are cyber warfare, cyber espionage and cyber crime[12]. The purpose of cybercrime is to gain material benefit using IT systems; its targets can be both business and political actors. The cyber espionage means the intelligence activities of states or market players carried out on IT tools, whereas cyber warfare occurs in case of conflicts between states, in which

conventional warfare is supported (or triggered) in order to render the information systems of the opponent state completely inoperative.

Fig 1. Types of Cyber Threats [12]

Cyber Terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not [10]. The various organizations involved in cyber terrorism are Al Qaeda, Council of Europe and Islamic State in Iraq and Syria (ISIS).

III. Evolution of Cyber Terrorism

All Cyber terrorism can be assumed to have started from June 1944 when attack was executed on the communication lines and logistic support of Germany. Since 1945, with the end of Second World War to 1991 the two super powers had emerged. They started to encroach and influence other nations through their dominant military force. It is known as cold war. The two 'super powers' were (1) the United States of America (USA) and (2) the Soviet Union[11].

By that time in 1960s to 1980s hackers took their own shape in Information Super Highway, in 1986, West German hackers accessed Department of Defense Systems of the USA. In 1988 Osama Bin Laden established 'AL-Qaeda' based on 'Jihad'. Thereafter, 'Gulf War' was first Information War or I-war through Information Way or I-way. The USA passed the National Infrastructure Protection Act, 1990 to control cyber terrorism. In Europe the I-way become popular in the year 1998. The United Kingdom (UK) established the Defense Evaluation and Research Agency in the year 1998. Then Sweden, Norway Finland, Switzerland, Germany, France came forward to combat cyber war.

By 1990 Internet became popular through World Wide Web (WWW). World Wide Web become very popular in India in 1995 but before that LTTE groups work was depend on website and Internet. In the era of information and communication technology almost all countries internet networks, fax networks and radio waves were notified about the possible conspiracy programme of terrorists against government. In India LTTE group's works depend mostly on network, websites and internet connectivity. Aftab Ansari's attack on American Centre, Kolkata was based on their organization through internet and websites. Even from Dubai he was able to communicate with his group. Therefore, in the contemporary communication convergence era cyber terrorism has become the most complex and national as well as an international problem.

Terrorists have moved into cyberspace to facilitate traditional forms of terrorism such as bombing. They use the Internet to communicate co-ordinate events and advance their agenda. While such activity does not constitute cyber terrorism in the strict sense, it does show that terrorists have some competency in using the new information technologies

Further terrorist are now drifting their interest into social networking sites. The role of social media can be identified indirectly in the cyber warfare as the infection of IT tools by malicious software, which is called computer-networking operations. These operations serve two purposes. On the one hand, they are used for network detection, and gathering information, on the other hand, modifying,

interfering, destroying the gathered information or achieving dysfunction in networks. [05]
The terrorist groups like ISIS have used social media sites for fulfilling following purposes:
• Obtaining information;
• Social engineering;
• Contacting;
• Propaganda;
• Recruiting new members;
• Receiving supporters;
• Committing psychological operations;
• Cyber-attacks.

Cyber terrorism is also expanding and off springing into industrial field, military and civilian domain, financial fraud, medical fraud, identity theft and many other forms of secret expression.

One of the aims of a terror attack is to draw attention of world to the terrorist group. However their propaganda could have different purposes like increasing the popularity of the terrorist group by the news describing their attacks, representing their declared purposes. It will also help in increasing the strength of the terrorist group.

IV. Social Media and Terrorism

Social networking sites have become a part of our daily lives: the inevitable parts of homes, workplaces, schools and leisure. Social media can be assumed as the combination of the web pages and applications that are used to share the contents on social network. They are providing a quick and easy sharing and dissemination of information among groups and communities. To propagate some agenda or to create negative awareness among peoples, these sites are favored.
Apart from common people, social media is also attracting terror groups as social media tools are cheap and accessible, facilitate quick, broad dissemination of messages, and allow for unfettered communication with an audience without the filter or "selectivity" of mainstream news outlets.[2]
Since social media proposes the right to express thoughts .So, terrorists are exploiting these social media platforms to plan their cause of terror, recruit, raise financial funds, distribute propaganda and communicate securely with other terrorists of different organizations and the different country without having to move anywhere. The terrorist organizations also use the web to reach out to their audiences and sympathizers without using other media such as radio, television or holding various press conferences. Not only this, such websites and web pages designed by these terrorist organizations often contain information and instructions on how to make explosives and chemical weapons. It also makes easy for them to identify the most common users that can have sympathy for them and also this is an effective method for recruiting new members to their terrorist organization. People access multiple social media channels regularly, most use Facebook (82%), YouTube (75%) and Instragram(53%).

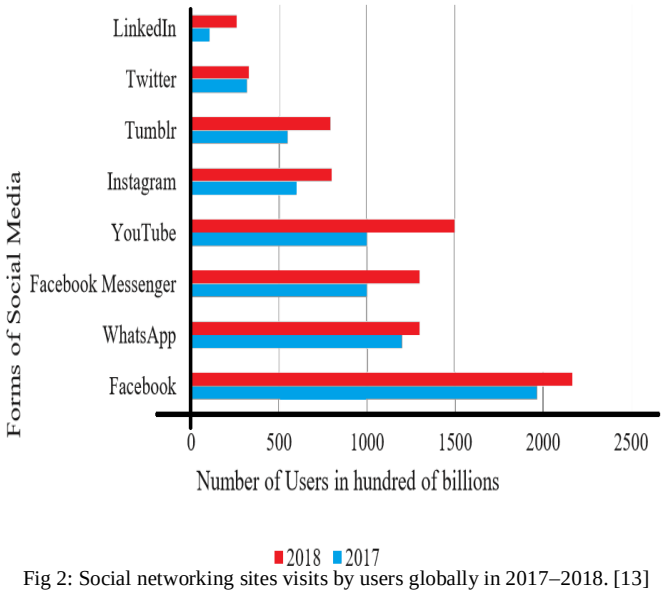

Fig 2: Social networking sites visits by users globally in 2017–2018. [13]

The terrorist activities through social media can be visualized in the forms of malwares that are used along with links and videos infected by malware codes and are used for campaigns or for spreading massive infection.
The features of the malwares expanded on social media platforms such as Facebook are the followings:

- we get message from our friend in a foreign language that he does not speak;

- link or video promising erotic content about a celebrity or about ourselves;
- our friends tag us in a bulk at a shared content;
- abbreviated link promising the above-mentioned contents or any other sensation;
- content promising huge discounts (e.g. branded sunglasses for some dollars, etc.).

The computer infected by any of these means can be used as:

- as a member of a botnet network, which can further be used by the attackers for mining crypto currency, sending spams or DoS attacks;
- ransomwares can be placed on our device that encrypt our files;
- can give access permissions to our system;
- spywares can be placed on our devices.

Many authors have proposed that media attention increases perceptions of risk of fear of terrorism and crime and relates to how much attention the person pays to the news.[03] The relationship between terrorism and the media has long been noted.[04] Terrorist organizations depend on the open media systems of democratic countries to distribute their message and goals. In order to earn publicity towards their cause, terrorist organizations resort to acts of violence and aggression that deliberately target civilians.[04] This method has proven to be effective in gathering attention of the world.

V. PREVENTIVE MEASURES TO MINIMIZE SOCIAL MEDIA EXPLOITATION

It has been found in a study by Gabriel Weimann from the University of Haifa found that nearly 90% of organized terrorism on the internet takes place via social media.[09].The role of social media can be identified indirectly in the cyber terrorism through various IT tools such as Facebook, Twitter, and other social networking sites.

In the order to stop the exploitation of social media by terrorist group, some government officials have requested social media companies to stop hosting content of the terrorist organization. In particular, Joe Lieberman had appealed to social media companies not to permit terror groups to use their tools for propagating their agenda.[06] In the report titled "Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat" issued by Lieberman and the United States Senate Committee on Homeland Security and Governmental Affairs in 2008 illustrated that the internet is one of the "primary drivers" of the terrorist threat to the United States.[06]

In response to the news that Al-Shabab was using Twitter, U.S. officials have called for the company to shut down the account. Twitter executives have not complied with these demands and have declined to comment on the case.[07]

In January 2012, Twitter announced changes to their censorship policy, stating that they would now be censoring tweets in certain countries when the tweets risked breaking the local laws of that country.[08] The reason behind the move was stated on their website as follows:

As we continue to grow internationally, we will enter countries that have different ideas about the contours of freedom of expression. Some differ so much from our ideas that we will not be able to exist there. Others are similar but, for historical or cultural reasons, restrict certain types of content, such as France or Germany, which ban pro-Nazi content. Until now, the only way we could take account of those countries' limits was to remove content globally. Starting today, we give ourselves the ability to reactively withhold content from users in a specific country — while keeping it available in the rest of the world. We have also built in a way to communicate transparently to users when content is withheld, and why [08].

Other incident is when in January 2018, Mark Zuckerberg announced that they would modify Facebook in a spirit of fighting against fake news. The modifications would highlight the posts of our friends and overshadow news portals.

So it is clear that if social media companies will make their rules-regulation and policies in order to

stop the cyber terrorism then it can be achieved easily.

Therefore, the measures that can be used by the counter-terrorism organizations for prevention and remediation are:

- counterpropaganda;
- psychological operations;
- mapping networks;
- intelligence;
- communication monitoring;
- integration;
- monitoring, disqualifying, recruiting managers;
- trend analysis;
- education;
- recruiting supporters and experts;
- inducing political decision making.

Social media gives the chance for the users to develop their data and information sensitivity. We need to create campaigns not only to develop their awareness, but also to reduce the spread of different malicious software, which may cause cyber-attacks.

VI. Conclusion

At last it can be concluded that the traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature. In the age of information technology the terrorists have acquired an expertise to produce the most deadly combination of weapons and technology and have opted an easy way to misguide and prevail hate among communities through the means of social networking sites which if not properly safeguarded in due course of time, will produce a damage that would be almost irreversible and most catastrophic in nature. In short, world is facing the worst form of terrorism, popularly known as cyber terrorism and they should take serious steps to prevent its propagation. Thus, a good combination of the latest security technology and a law dealing with cyber terrorism is the need of the hour.

References

[1] [1] fbi.com: Tesimony of Keith Lourdeau, Deputy Assistant Dierctor, Cyber Division, FBI Beore the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security Februray 24, 2004.
[2] [2] Dark, Calvin (December 20, 2011). "Social Media and Social Menacing…". Foreign Policy Association. Retrieved April 5, 2012.
[3] [3] Nellis and Savage (2012).
[4] [4] Wilkinson, Paul (1997). "The media and terrorism: a reassessment". Terrorism and Political Violence.
[5] [5] ANDRESS, J., WINTERFELD, S.: Cyber Warfare (Second Edition). Techniques, Tactics and Tools for Security Practitioners. Waltham: Elsevier Inc., 2014.
[6] [6] "Joe Lieberman, Would-Be Censor". The New York Times. May 25, 2008. Retrieved April 5, 2012.
[7] [7] Friedman, Uri (December 20, 2011). "U.S. officials may take action again al-Shabab's Twitter account". Foreign Policy. Retrieved April 5, 2012.
[8] [8] "Tweets still must flow". Twitter. Retrieved April 5, 2012.
[9] [9] CBC (January 10, 2012). "Terrorist groups recruiting through social media". CBC News. Retrieved April 5, 2012.
[10] [10] Dorothy E. Denning, "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism", Committee on Armed Services, U.S. House of Representatives, Available on http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf, Retrieved on 12 March 2010.
[11] [11] Dr. M. Dasgupta, Cyber Crime in India-A Comparative Study, pp. 191-193, Eastern Law House, Kolkata, 2009.
[12] [12] KRASZNAY Cs.: A polgárok védelme egy kiberkonfliktusban. Hadmérnök, VII 4 (2012),142–151.http://hadmernok.hu/2012_4_krasznay.pdf (Downloaded: 18.03.2018).
[13] [13] Statista, www.statista.com