IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Terrorism in the Cyber Space: The New Battlefield

Saumya Gupta[1], Akhilesh Tiwari [2]

Research Scholar, Department of CSE & IT, Mits, Gwalior, India [1]

Associate Professor, Department of CSE & IT, Mits, Gwalior, India [2]

Abstract: Terrorism has become a global threat from the past few decades and needs to be controlled from the grass root level to the universal level. Internet technology makes it easy for terrorist groups to communicate with relative anonymity, rapidly and effectively across borders, to an almost illimitable audience. This emerged as a threat to nation's internal security therefore identification of terrorist groups on cyber space has become essential task in recent times. It is the task of determining associations and predicting the relationships that may exist between terrorist nodes. This has several applications including the recognition of terrorism, drug trafficking, gang related offences, frauds and armed robberies etc. There are two types of warfare in the world of terrorism: Conventional Warfare and Cyber Warfare. Conventional Warfare deals with the terrorism occurring on the four dimensions (land, sea, air & space) whereas Cyber Warfare deals with the 5th dimension i.e. Cyber Space. The use of the Internet space for terrorist purposes creates both challenges and opportunities in the fight against terrorism. This paper is a review on Cyber warfare as it has several benefits over Conventional warfare such as easier identification of crucial nodes & links; law enforcement agencies will get help and support to counter terrorism attacks.

Keywords: Data mining, Social connections, Social network analysis, Investigative data mining, Terrorist network mining, Terrorist using social media, Graph theory.

I. INTRODUCTION

The face of modish terrorism is different than the face of terrorism in the past. Traditionally, terrorist clusters were determined manually and a major disadvantage of this type of approach was the time and efforts it need to generate fruitful results [1]. But now as we entered into 21st century, technology is one of the strategic factors driving the growing use of the Internet by terrorist organizations. While many benefits of the Internet are unavoidable, it may also be used to promote communication within terrorist organizations and to transmit information, as well as material support for intended acts of terrorism, all of which require specific hi-tech knowledge for the effective investigation of these offences [2]. Due to these increasing terrorist activities it becomes important to restrict terrorism spread before it's too late. Therefore there is an immediate need to study the web based behavior of the criminal minded people to collect data on terrorist networks, examine such networks to find hidden relations and groups, detect key players, discover points of vulnerability, and find the efficiency of the network [3]. In 2007, N.Memon presented a new terrorism knowledge base, iMiner, by harvesting information from different sources. The author described the prototype for analyzing, visualizing and destabilizing terrorist networks. Furthermore, it has been illustrated that the proposed iMiner allows analysts to determine the hierarchy of covert networks, which would aid law enforcement agencies in understanding the structure of the terrorist networks and identification of important nodes in the network. In real sense, iMiner is an experimental system which reveals:

- Determination of the importance of a node.
- Connection among nodes (highly/less connected).
- Identification of various position roles in the network.
- Determination of nodes representing key players [4].

Law enforcement and intelligence agencies realized that knowledge about terrorist networks is important for the crime investigation and may be to a large extent, shape & direct the police efforts [14]. A clear & deep understanding of network structures and individual roles can assist law enforcement and intelligence agencies to develop effective strategies in order to prevent future terror attacks. However, except for network visualization, criminal network analysis remains primarily a manual process [15].

II. INTERNET: A WEAPON FOR TERRORIST ORGANIZATIONS

The Internet is a powerful weapon for terrorists, who use virtual message boards , groups, forums, and chat rooms to share information, organize attacks, spread propaganda, raise funds, and to recruit youth generation [12]. Terrorism organizations exploit these facets of the web in very efficient manner for their destructive plans [13].

According to a research it has analyzed that the number of terrorist sites increased exponentially over the last decade--from 100 to more than 4,800 two years ago. Hundreds of sister sites of terrorist groups have been promulgated but only a handful are considered active and these active

DOI 10.17148/IJARCCE.2016.5552

websites can serve as virtual training grounds, offering tutorials on building bombs, firing surface-to-air missiles [12]. The website has links to legal files on terrorist suspects which makes it a very precious resource for researchers [5].

III. 'TERRORIST WEBSITE': A SOURCE OF INFORMATION

Describing a terrorist website is as contentious as defining terrorism [12]. Today, almost all active terrorist organizations maintain their websites regularity and many maintain more than one website and use several languages [6]. Terrorist sites include the official sites of designated terrorist organizations, as well as the sites of supporters, sympathizers, and fans [12]. Website also contains audio, video files to enhance the presentation of their message. Terror organizations capture information about the person who browse or visit their website [7]. Typically, a site will provide a history of the terror organization and its activities, a detailed review of its social and political background, accounts of its notable exploits, information of their leaders, founders, and heroes, information on its political and ideological aims, fierce criticism of its enemies, and also up to date news. Most sites do not feature is a detailed description of their violent malicious intentions [6]. Frequent site outages, however, make it difficult to track their content and sentiment [3]. This explosively emerging, extensively available, data makes our time truly the data age. This huge amount of data created and available has laid the data mining as an emerging tool for detecting and preventing terrorism [8].

IV. DATA MINING

The Internet may be viewed as a vast digital bibliotheca. The World Wide Web alone offers about a billion pages of information, much of it free of cost — and much of it of interest to terrorist organizations [9]. A large amount of general information is available on the internet, including publicly available maps and building details that could be searched for by a person planning a terror attack.

Huge numbers of tools are available to facilitate such data collection, including search engines, chat rooms and discussion groups. Many websites offer their own search tools for fetching data from databases on their sites [6].

Data mining is seen as a most prominent technique for decision makers to make decision, discovering hidden relation and pattern, foreshowing possible behaviors' which may occur in the future by analyzing historical and current data.

V. SOCIAL CONNECTIONS

The practice of investigating for underlying connections or social connections between people in data mining is called social network analysis. Web data is useful because it helps to describe relationships and associations among different groups. With social network analysis, contacts are commonly set out graphically to demonstrate connections and find patterns. At the simplest level, to understand networks and their participant's players, we evaluate the position of actors in the network. Measuring the network position is finding the centrality of a node in cluster. These measures offer an insight into the various roles and groupings in a network -- who are the connectors, leaders, bridges, isolates, where the clusters in the network and who is in them. Social network researchers use the concept of Degree in order to measure network activity for a node – Degree is the number of direct connections a node has. Node which has the most direct connections in the networks is referred as the most active node in the network. That active node is a 'connector' or 'hub' in this network.

VI. SOCIAL NETWORK ANALYSIS

Social network analysis or social network investigation in general studies the behavior of the individual at the micro level, the template of relationships (network structure) at the massive level, and the interactions between the two [17] with the use of graph theories and network. It describes the networked framework in terms of nodes (individual actors, people, or things within the network) and the edges (relationships or interactions) or ties that connect them. A social network is usually interpreted by a graph, since graphs provide an innate idea of how the network is constructed and it is easy to analyze using mathematical methods and software tools.

SNA can be used to deduct useful information from a social network, such as:

- Analyzing information passing through the network,
- Scope of information reach or spread within the network when propagated by a given node
- Identifying specific paths taken by the information to move from one node to another,
- Discovering non-obvious relations between actors, and
- Identifying nodes that are directly or indirectly associated to most other nodes in the social network [19].

These analysis techniques can classify individuals into a number of groups based on their attributes (for example friendship, common interest, financial exchange, beliefs, knowledge or prestige) in order to model real world interactions within the network. When the relationships and information of flow become visible, then useful information can be deduced from the graph. This information can help to improve or even freeze information propagation within the network.

The overall contribution of social network analysis to counter terrorism is the ability to map the invisible dynamics inside a terrorist community.

The use of social network analysis in the widespread has increased with the growth of a number of new online web sites based on social network principles.

DOI 10.17148/IJARCCE.2016.5552

VII. INVESTIGATIVE DATA MINING

Data mining is appropriate for decision makers to make decision, discovering hidden relation and pattern, foreshowing possible behavior's which may occur in the future by analyzing historical and current data. When the SNA is applied for investigating of terrorist arrangements or networks on web then it is recognized as Investigative Data Mining (IDM), also known as Terrorist Network Mining/Dark Network [8]. The main focus of IDM approach is to identify important actors, crucial links, subgroups, network characteristics, roles and so on, to answer substantive questions about terrorist organizational structures [18].

VIII. TERRORIST NETWORK MINING

Terror is a very complicated word in the political and security world [19]. Relationships between terrorists form the basis for the coordinated crimes. TNM is the process of posing questions and digging out useful information from enormous amount of social communications using various known techniques [11].

IX. TERRORIST USING SOCIAL MEDIA

Social media is a key element of modern terrorism. Due to the accessibility, affordability, and broad reach of Social platforms such as YouTube, Facebook, Myspace, Twitter, and Tumblr, terrorist groups have increasingly used social media to fulfill their malicious objectives and broadcast their message within the borders of country and outside. Attempts have been made by a range of governments and agencies to foil the use of social media by terrorist organizations. Today, about 90 per cent of systematic structured terrorism on the internet is being carried out through social media. By using social media as a tool, the organizations are able to be active in recruiting new friends without geographical restriction. The social media is facilitating the terror organizations to take initiatives by making "friend" requests, uploading video clips, and audio messages. Like most social networking sites, Twitter prohibits activity if users post direct, specific threats of violence against others but the problem is that doesn't actively monitor the content in search of the above threats. Instead, it relies on users to report in case they notice violations to the rules.

X. GRAPH THEORY FOR THE SOCIAL NETWORK ANALYSIS

The Graph theories are used to create the nodes which will help in the analysis for the network. Basically, the graph is the collection of nodes (n) and the edges (e) such that e = (ni, nj) where ni and nj are any two connected nodes. When graph theory is used to personify the social network then such graph is called a socio graph, where nodes are the actors and edges are the lines of connection between these actors. The socio gram can be both unidirectional as well as directional.

There are a range of concepts of graph theory like closeness in between the actors, position of prestige, centrality etc. which can be applied in the investigation of social networks.

- Degree: Number of direct connections that a node has.
- Between ness: The number of path that connect pairs of nodes that travel through a given node.
- Prestige: A measure of links to other highly central node.
- Closeness: The number of other nodes that are associated to a given node.

These specifications have calculated indices based on matrix graph with direct network implementation.

An entity with the high degree index means that it is very strongly networked or active. An entity with a high between ness index would have a strong "vigorish" role. A centralized network with a very high Degree index in one or few nodes can become a single point of failure. A less centralized arrangement would be flexible in the face of collapse or failure; it would experience graceful degradation [11].

XI. DESTABILIZING TERRORIST NETWORKS

Destabilizing approach traditionally intend at neutralizing members of terrorist networks either through capture or demise. The removal of a node from the system can make a cell less capable to adapt, reduce its performance, and reduce its ability to communicate. These nodes are known as the 'critical' nodes inside a network. The removal or isolation of these nodes ensures maximum damage to the network's ability to adapt, performance, and ability to communicate [18]. Using standard social network techniques, individuals who are key in the terrorist networks are identified and then removed. The argument is that their removal serves to weaken or split the network so that messages flow slower and so that the network as a whole is no longer a single entity [22].

XII. LITRATURE REVIEW

1. S.Maheshwari et.al. presents work which is carried out in two stages. The initial stage presents Genetic based optimization mechanism for effective optimization of large social network containing of terrorist and non-terrorist nodes. In the optimization procedure removal of non-terrorist nodes from the network has been done and resultant is a minimize graph containing only the set of potential nodes. The next and the final stagepresents a weighted degree centrality measure for effectively neutralizing of the terrorist network [8].
2. N.Chaurasia et.al. examined various methods for identifying terrorist activities using social network analysis [16].
3. Nasrullah Memon et.al. presents the study of structural cohesion which is analyzed in Social

DOI 10.17148/IJARCCE.2016.5552

Network Analysis, but can also useful in other important application regions including investigative data mining for destabilising terrorist networks. Structural cohesion is the number of actors who, if detached from a group, would disconnect it. They have also discuss about the structural cohesion concepts, such as cliques, n-cliques, n-clans and k-plexes to determine familiarity, robustness and reach ability within subgroups of the 9/11 terrorist association [17].

4. Muhammad Akram Shaikh et.al. presents an to perception that how IDM works and the significance of this approach in identifying key nodes in terrorist networks [18].
5. AlaBerzinji study decentralized terrorist networks with different variety of nodes. The nodes can be organizations, places or individuals. We use a composition of different centrality measures to detect key players in such network [19].
6. Chintan Dave et.al. presents methodology that learns the unusual behaviour of terrorists by applying a data mining algorithm to the textual content of terrorist related data . The outcome of an initial case study express that the scheme can be useful for detecting terrorists and their supporters using a authorized ways of Internet access to view terrorist related content at a series of evasive web sites [20].
7. Kathleen Carely et al. demonstrated the clear benefit of military relevant social network analysis (SNA) models to quickly and economically illustrate destabilization strategies against covert networks [21].

XIII. MILITARY AND ITS WAR ON CYBER ATTACKS

The military is also modifying how to respond and train brigades when it comes to cyber warfare. Facebook and other social media’s are also being used by the terrorist organizations to collect military related confidential information. Numerous military users don't even trouble finding out who they are confirming as 'friend' and to whom they are providing entrée to a large amount of information on their personal life, so it becomes important to train the military peoples. The terrorists built false profiles that facilitate them to get into highly visible groups. Countries such as the Canada, U.S. and the U.K. have instructed their military persons to remove personal information from Facebook in case al-Qaeda is monitoring it. Military continues to advance their approach to handling cyber security; jobs in cyber warfare have become increasingly popular in the military area. The United States Navy strongly & actively recruits for cyber warfare engineers. The US Army & other country army has their Cyber Command where they ardently recruit for cryptologic network warfare specialists.

XIV. LURE OF YOUTH INTO TERRORISM

Internet and youths are so closely intertwined which makes internet a useful tool particularly in reaching out to the youth. Structured and deliberate plans have been made by terrorists to radicalize and recruit young people into committing acts of violence. Terrorist organizations are recruiting and influencing youths to carry their dastardly acts in the name of God or religion. Youths are used by terrorists to be recruited because they have no prior police records, so involvement of youths would reduce the chances arrest of the more senior terrorist leaders [10]. It is easy for them to train the young blood as the training involves a lot of mental stability, physical exercise, and determination. Youths are sometimes given more dangerous tasks as if they are caught they would receive lighter sentences or relaxation due to their age.

XV. ADVANTAGES

1. This system will help to reduce terrorism spread around the world.
2. This system will help anti-terrorism division/agencies.
3. This system helps law enforcement agencies to detect suspicious web pages or nodes and track them.

XVI. DRAWBACKS

[1] Privacy Concerns

Data mining is nowadays used for detecting & preventing from the terrorist activities but also cause some privacy concerns, Data mining tools that are easily available on the web can be used by the notorious individuals to extract information of some person from the data stored on the databases [11].

[2] Youth Concerns

Due to a large involvement of youth by terrorists, it may be possible, that the next battlefield in the fight against terrorism will not take place on a physical plane but in the mental and emotional domains of the youth, and this will cause a major destruction for our nation, as youth are present &future of our country [10].

XVII. CONCLUSION

Terrorists conduct wars in cyberspace as well as on the land. Cyber Space in certainly a new area of a battlefield. Since 9/11, terrorists sharpened their internet prowess and increased their presence on the web. History has proven that terrorists groups exploit new technologies to plan attacks and learn from their mistakes, and take advantage of law enforcement’s misjudgments in their emerging capabilities to carry out deadly attacks. As we are seeing, one of the major concerns of our nation today is to detect and prevent terrorist attacks. In this paper, we have presented an overview of investigative data mining with its basic framework and tried our best to shed some light on the issues. We believe that investigative data mining has an assuring future for increasing the effectiveness and efficiency of counter terrorism and intelligence analysis. Identification & Destabilization of the Key Player Node in the terrorist network will help and support law enforcement agencies to counter terrorism attacks.

DOI 10.17148/IJARCCE.2016.5552

REFERENCES

[1] N.Chaurasia, M. Dhakar, A.Tiwari and R. K. Gupta, "A Survey on Terrorist Network Mining: Current Trends and Opportunities", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.4, August 2012.

[2] United Nations Office on Drugs and Crime Vienna, "The use of the Internet for terrorist purposes", United Nations publication, V.12-52159—September 2012—350.

[3] Nasrullah Memon,"Detecting Hidden Hierarchy of Non Hierarchical Terrorist Networks", Third International Conference on Mathematical Methods in Counterterrorism .

[4] N.Memon,Henrik,legindLarsen,"Investigative Data Mining Tool Kit:a software prototype for Visualizing,Analysing and Destabilising Terrorist Networks", InProceedings of Visualizing Network Information,pp. 14-1 – 14-24(2007).

[5] Albert J. Jongman, "Internet Websites and Links for (Counter-) Terrorism", Terrorism Research Initiative, ISSN 2334-3745.

[6] Gabriel Weimann,"How Modern Terrorism Uses the Internet".

[7] B.Ganor, Knop, Carlos," Hypermedia Seduction for Terrorist Recruiting".

[8] S.Maheshwari and A.Tiwari ,"A Novel Genetic Based Framework for the Detection and Destabilization of Influencing Nodes in Terrorist Network", Computational Intelligence in Data Mining – Volume1,Smart Innovation,System and Technologies Vol. 31,pp. 573 -582,2015. (DOI 10.1007/978-81-322-2205-7_53) Published in Springer.

[9] Gabriel Weimann ,"Terror on the Internet: The New Arena, the New Challenges".

[10] Thomas Koruth Samuel,"The Lure Of Youth Into Terrorism".

[11] R.D Gaharwar, D.B Shah, and G.K Gaharwar ,"TerroristNetworkMining:Issuesand Challenges",IJARSE,VOL. No.4,ISSN-2319-8354.

[12] Eben Kaplan," Terrorists and the Internet", council on foreign relations.

[13] Jayanthi, S.Sasikala,"XGraphticsCLUS: Web Mining Hyperlinks and Content of Terrorism websites for Homeland Security" Int. J. Advanced Networking and Applications 941 Volume: 02, Issue: 06, Pages: 941-949 (2011)

[14] Macandrew, D. 1999. The structural Analysis of criminal networks. In The Social Psychology of Crime: Groups, Teams and Networks. D. Canter and L. llison, Eds. Dartmouth Publishing, Aldershot, UK, 53-94.

[15] Xu Jennifer,Chen Hsinchun 2005. ACM Transactions on Information Systems. Vol. 23,No.2,201-226.

[16] N.Chaurasia, M. Dhakar , A. Chharia, A.Tiwari and R. K. Gupta ,"Exploring the Current Trends and Future", Academy & Industry Research Collaboration Centres ,CSCP vol2 csit2238, PP 378-385.

[17] NasrullahMemon," Structural Analysis and Destabilizing Terrorist Networks".

[18] Muhammad AK ram Shaikh and Wang Jiaxin," Investigative Data Mining: Identifying Key Nodes in Terrorist Networks", Multi topic Conference, 2006. INMIC '06. IEEE [ISSN 1-4244-0795-8].

[19] AlaBerzinji," Detecting Key Players in Terrorist Networks", UPPSALA UNIVERSITET.

[20] Chintan Dave Anil Prajapati, "Using Data Mining Techniques to Track Terror Activities on WEB". Carley M. Kathleen, Lee Ju-Sung, David Krackhardt.2002. Destabilizing Networks. Connections 24 (3) 79-92. Carley M. Kathleen, Lee Ju-Sung, David Krackhardt. 2002. Destabilizing Networks. Connections 24 (3) 79-92. Carley M. Kathleen, Lee Ju-Sung, David Krackhardt. 2002. Destabilizing Networks. Connections 24 (3) 79-92.

[21] Carley M. Kathleen, Lee Ju-Sung,David Krackhardt.2002.Destablizing Networks.Connections 24(3) 79-92.

[22] Jennifer J. Xu and Hsinchun Chen. CrimeNet Explorer: A Framework for Criminal Network Knowledge Discovery, ACM Transactions on Information Systems, Vol. 23, No. 2, April 2005, Pages 201-226.

DOI 10.17148/IJARCCE.2016.5552