

Friend of a Friend Influence in Terrorist Social Networks

Todd Waskiewicz

Air Force Research Laboratory, AFRL/RIEA

525 Brooks Road, Rome, NY 13441-4505

todd.waskiewicz@rl.af.mil

Abstract – *With the increasing popularity of social media over the last few years, terrorist groups have flocked to the popular web sites to spread their message and recruit new members. As terrorist groups establish a presence in these social networks, they do not rely on direct connections to influence sympathetic individuals. Instead, they leverage “friend of a friend” relationships where existing members or sympathizers bridge the gap between potential recruits and terrorist leadership or influencers. As anti-Western propaganda flows through these social networks, homegrown terrorists and lone wolf terrorists have been inspired to commit acts of terrorism. These terrorist social networks in social media can be uncovered and mapped, providing an opportunity to apply social network analysis algorithms. Leveraging these algorithms, the main influencers can be identified along with the individuals bridging the gap between the sympathizers and influencers.*

Keywords: terrorism, terrorist networks, social media, influence, social network analysis

1 Introduction

Terrorists use a number of methods to indoctrinate and radicalize new followers. With the growth of the Internet and the explosion in popularity of social networking sites all over the world in recent years, terrorist groups have significantly increased their global reach. They are now able to spread propaganda and recruit half way around the world from the convenience of an Internet café. Terrorist groups and their members have made a concerted effort to increase their presence on social media sites like Facebook and Twitter to go along with their existing Internet presence on web sites, forums, and message boards. However, it is their new found presence on social media sites that allows them to identify and target individuals that are particularly influenced by their propaganda. By reaching out to disillusioned individuals, they attempt to create new followers. The ultimate goal is to indoctrinate and radicalize these people so they feel compelled to commit acts of terrorism.

The individuals that have become indoctrinated with terrorist ideology have been heavily influenced during their use of social media. This has especially been the case with homegrown terrorists that have committed acts of terrorism in Western countries. Although they never had direct access to the terrorist ideology or training camps, they were exposed to

it through relationships developed on social media sites and subsequently influenced. However, it was not necessarily the direct connections within their social networks that were the heavy influencers pedaling terrorist ideology. Often, it comes from individuals they are not directly connected to, but someone they encounter through a direct connection or “friend.” Through a “friend of a friend,” a disenchanted individual can quickly become enamored with the anti-Western culture. Consequently, it is important to identify these at risk individuals, the influencers, and the bridge between them. A variety of social network analysis methods can be used to identify these actors within a social network. This paper will explore terrorists’ use of social media and the phenomenon of “friend of a friend” influence. Furthermore, it will discuss social network analysis techniques aimed at discovering these entities within social networks.

2 Terrorists’ Use of Social Media

Over the last ten to fifteen years, the presence of terrorist groups online has greatly increased. In 1998, there were only 15 web sites associated with terrorist groups on the Internet [1]. By 2005, there were more than 4,000 [1]. Up until recent years, terrorists have limited themselves to more covert means of communication on the Internet such as password-protected forums for communicating and disseminating propaganda to support their causes. There was a shift in the way terrorists conduct operations. In an effort to adapt with current technology trends and reach larger audiences with their message, they have taken up the use of social networking sites. These sites also provide a number of other benefits as terrorists attempt to spread their propaganda. With that being said, terrorist groups are using social networking sites as a new medium for recruitment, radicalization, and planning.

In December 2008, pro-jihad contributors to the “al-Fajola Islamic Forums” urged Al-Qaeda supporters to “invade” Facebook by creating sympathetic groups to spread the Salafi-Jihadi message [1]. This movement had almost immediate results. In December 2009, Pakistani authorities arrested five young American Muslims as they were attempting to join Al-Qaeda [2]. Groups such as Lashkar-e-Taiba and Lashkar- e-Jhangyi used Facebook and YouTube to recruit them [1]. In regards to this incident, a high-ranking Department of Homeland Security (DHS) official said, “Online recruiting has exponentially increased, with

Facebook, YouTube, and the increasing sophistication of people online” [2].

There are many motivating factors behind the migration of terrorists to social networking sites. Terrorists have always utilized the latest technology to support their cause. Examples include the use of complex encryption programs for communications and altering computer games to mimic real life missions and attacks. As a result, their use of social networking sites is a natural progression of their technology-oriented tactics. Terrorist organizations have also moved to social networking sites out of self-perseveration [3]. Traditional web sites hosted by an ISP are prone to monitoring, attacks, and subject to shutdowns. Terrorist web sites are always targeted by the United States and its allies. Patriotic hackers also target the web sites using distributed denial of service (DDoS) attacks. For example, in June 2011, a hacker named “The Jester” shut down <http://www.alijahad.com> [3]. If they use a Facebook page, there is a very low probability someone would execute a DDoS attack against Facebook’s web site. That is even assuming they can locate the page in question. The use of social networking sites provides terrorists with free web hosting where they can upload content anonymously, reliably, and at no cost [4].

Social networking sites are attractive to terrorists and their groups because they have features to control access to the page [5]. Instead of the site being open to the public, the page owner can set it to private. Then the owner must approve someone’s request for access or invite them to join the page. This provides the opportunity to vet an individual thoroughly before granting them permission to view the content of the group’s page or participate in a discussion forum [5]. Additionally, the owners can monitor the content posted on the pages. This provides a unique environment for terrorists where they control the content and access to it while also reaching large audiences.

The most important reason terrorist organizations are taking to social networking sites is to recruit, indoctrinate, and radicalize new members that can support their cause. “The Internet is the enabler that acts as a catalyst for the radicalization lifecycle” [6]. Without the use of the Internet and social networking sites, the perpetuation of Al-Qaeda’s message would be severely stifled [6]. However, the radicalization process that used to take months now takes weeks or even days [6]. With the help of the Internet, terrorists are able to communicate across the globe instantly. They are targeting mainstream social networking sites because they are more accessible to sympathizers than the hardcore forums [7]. After the indoctrination of sympathizers, they are steered to the terrorist forums where some will finally join the front lines of the jihad [7].

3 Friend of a Friend Influence

A “friend of a friend” is described as an individual that has a friendly relationship with the friend of a person, but that person has no direct relationship to that individual. Figure 1 depicts the friend of a friend relationship between nodes A

and C in the social network. C is a friend of A’s friend B, and vice versa. A and C are not directly connected, but a path exists between them through C. Although there is no direct

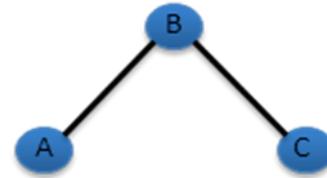


Figure 1. A friend of a friend relationship between A and C

connection between the person and the friend’s friend, this is still an important relationship. Each person can exert a certain amount of influence on one another using the common friend as an intermediary. Ideas, information, behavior, and even feelings can spread through this social network. In addition, when the flow of information and ideas are strong enough, the three individuals will form a triad. In fact, social theory even argues there is a strong propensity for people to form these triads. Once this direct connection is formed between the two individuals that were not previously directly connected, ideas, information, and behavior are free to flow back and forth. The triad formed by A, B, and C is shown in Figure 2. This is the exact social phenomenon that terrorists are looking to exploit when using social media sites in an effort to build their virtual networks.

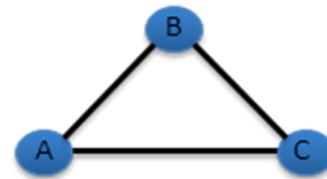


Figure 2. A triad formed between A, B, and C

4 Terrorists’ Use of Friend of a Friend Relationships on Social Media Sites

Initially, the terrorists’ first attempts at infiltrating social media sites like Facebook consisted of “Facebook raids” or campaigns aimed at disseminating their propaganda through existing Facebook channels [8]. Although this was spreading their message, it did very little in the way of adding followers and building their virtual networks. Their subsequent efforts have been to establish a permanent presence on Facebook by creating groups and virtual communities affiliated with terrorist web sites [8]. This allows the terrorists to bridge the gap between sympathizers and leadership. This is where the friend of the friend relationship starts to take root. To reach out to the Facebook users they are trying to recruit, terrorists are creating Facebook pages and coordinating communication between Facebook and the web sites. The terrorists operating on Facebook befriend sympathizers on the fringe and begin pedaling their anti-Western sentiment. This forms the structure seen in Figure 1 and starts the information flow from terrorist leaders and web sites to the sympathizer.

Information also flows back through this channel as sympathizers are often afforded the opportunity to interact with leadership through the intermediary. The flow of information will continue as the sympathizer becomes indoctrinated and radicalized, eventually leading to the individual becoming vetted and accepted as one of them. They then gain access to the password protected forums and web sites and are allowed to interact directly with leadership, effectively closing the triad and forming the structure depicted in Figure 2. This is the best case scenario terrorist groups hope for when targeting social media sites for new members. There are many examples that show terrorist groups attempting to reach out to sympathizers on social media sites. Some are clear cases that illustrate a concerted effort to bridge the gap between leadership and sympathizers and others show individuals that have been radicalized through these means and motivated to carry out acts of terror.

Many consider the Facebook page Jihad Al-Ummah to be one of the most important terrorist pages on Facebook and one of the most authoritative sources on the Internet outside of the actual forums [8]. The page is closely associated with the Shumukh Al-Islam forum and is a hub for jihadi material [8]. It distributes content from terrorist sites and serves as a liaison between Facebook users and those same sites [8]. The Jihad Al-Ummah Facebook page contains videos, announcements, articles, and other jihadist media right after it appears on the Shumukh forum [8]. To facilitate the material's dissemination through Facebook, they will tag friends of the page in the posts [8]. This brings the newly posted material to the attention of friends of the page or friends of the friends as they are updated on their friend's Facebook activity. For example, the Shumukh forum announced an open question and answer session with Sheikh Abu Walid Al- Maqdisi, leader of a Gaza based jihadi group [8]. Jihad Al-Ummah's Facebook page also announced the session and collected questions written by friends of the page [8]. Those who ran the Facebook page then passed on the questions to the Shumukh forum for answering. The friend of a friend relationship is being exploited by connecting friends of the Jihad Al-Ummah Facebook page to leadership in an effort to influence sympathizers. Utilizing Facebook in this manner for communications allows terrorist organizations to insulate leadership while also providing access for sympathizers.

The same type of activity is also reflected on Twitter. Twitter pages are set up to notify followers of updates on terrorist web sites and blogs. The Twitter page serves as the intermediary between sympathizers and the terrorists behind these web sites and blogs. The Taliban attempts to use Twitter in this manner. They leverage a system called TwitterFeed that automatically updates a Twitter page to reflect web site or blog updates [9]. Anytime there is a new addition to the web site, a link to the update is tweeted. This instantly updates followers who receive the tweet. The followers are now able to go directly to the site to view the update, bridging the gap between the propaganda and sympathizers.

Utilizing these communication patterns in social media, terrorists groups have inspired homegrown terrorism and

driven seemingly normal individuals to act in support of their cause. For example, Taimour al-Abdaly appeared to be an average family man. He was a former DJ from Great Britain that was married with three children. However, much more sinister intentions were developing underneath his outwardly appearance. In December 2010, on a suicide mission, he blew himself up in Stockholm, Sweden, injuring two others.

As it turns out, he was a member of a virtual terrorist network constructed through social media. After the fact, when researchers explored Taimour's social media activity, they determined there were only three degrees of separation between him and Samir Khan [7]. Khan was one of Al-Qaeda's top media operatives before being killed in Yemem as the target of a U.S. drone attack in September 2011. Figure 3 shows the friend of friend relationships that existed between them with Taimour's friend being friends with several of Khan's friends [10]. Khan and his friend were not the only

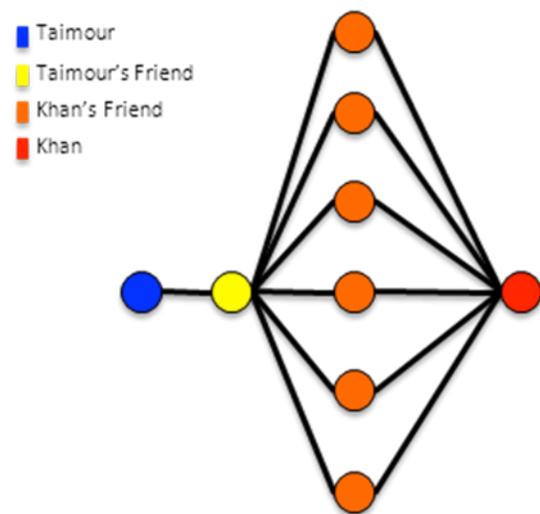


Figure 3. Subset of Taimour's Social Network

individuals who Taimour encountered online. His social media exploits also extended to YouTube where he would frequently view YouTube videos that consisted of violence and anti-Western propaganda. In fact, he was connected to Mohammed Gul, who was sentenced to jail in February 2011 in Britain for posting extremist Islamic material on the Internet. Taimour labeled four videos posted by direct associates to Gul as his favorites on YouTube [11].

Another individual that was heavily influenced by their involvement in virtual terrorist networks is Arid Uka, who opened fire on U.S. soldiers in Frankfurt, Germany, killing two and wounding another two. On Facebook, Uka had 127 friends that included extremists such Salahudin Ibn Ja'far [12]. Ja'Far openly identified with Germans involved in terrorist activity and was strongly linked as a friend and subscriber of two YouTube accounts known for posting extremist propaganda [13]. Uka was also Facebook friends with a German jihadist group using the name "Dawaffm De" that was friends with "AzeriJihadMedia," a jihadist media organization, on YouTube [14]. Uka was never a known member of any terrorists groups and was not under any type

of surveillance before his attack [15]. He was simply immersed in this online terrorist social network. Given his connections to extremists and their connections to others, it is clear that anti-Western propaganda flowed through this network and heavily influenced him. So much so that he decided to commit an act of terrorism and murder two U.S. soldiers.

5 Using Social Network Analysis to Detect Friend of a Friend Activity

It is clear that in online terrorist social networks influence is flowing through friends and between individuals who are not even directly connected, radicalizing extremist sympathizers with no physical connections to terrorist groups. Since a specific behavior has been established with these virtual networks, we can begin to use social network analysis methods to disrupt the flow of influence and try to prevent individuals from becoming indoctrinated with extremist ideals. Mapping the relationships between members of these online terrorist communities creates a social network. Various social network analysis methods can then be used to identify the different individuals that are a part of these types of relationships.

If there is an individual that is a part of a social network and feared to be a terrorist sympathizer, their ego network analysis will identify the individuals with whom they are connected to and influenced by. Ego network analysis consists of analyzing an individual within a social network and all the nodes the individual is connected to at some path length [16]. According to social theory, influence works at distances with up to three intermediaries [3]. Identifying all persons with a path length of 2 from ego produces a list of all of their friend of a friend relationships. This could go on to path lengths of three and four to identify further influencers and intermediaries. Figure 3 is essentially a subset of Taimour's ego network, depicting the people he is connected to with path length three or less. The people found to be on the end of these paths are potential influencers while those found in between are the intermediaries passing it along. Ego-networks can also be examined for structural holes. A structural hole refers to a tie that is absent [16]. For example, the network depicted in Figure 1 has a structural hole between A and C while Figure 2 contains no structural holes. Social network analysis software such as UCINET analyzes ego networks for structural holes. Identifying structural holes may lead to the discovery of friend of a friend relationships in which influence is flowing from terrorist leadership to sympathizers.

Betweenness centrality measures the ratio of shortest paths an individual is present upon. Individuals with a high betweenness centrality hold a very important position in a social network. By being present on the shortest path between two individuals, they have the opportunity to serve as a broker of information by passing it along or affecting it in some way. In the friend of the friend relationship, they serve as the intermediary connecting two individuals that would otherwise be disconnected. For example, in Figure 1, B would

score a high betweenness centrality for being on the shortest path between A and C. By calculating the betweenness centrality for an entire social network, the individuals with the highest betweenness values are identified. By the pure definition of betweenness centrality we know that these individuals must be connecting others who are not directly connected. As a result, by using betweenness centrality, we identify the individuals in the friend of a friend relationships that are passing information and influence between terrorist leadership and sympathizers in social networks.

Community detection algorithms detect groups that exist within social networks and help reveal network structure. Most community detection algorithms work by measuring the density between sets of nodes and identifying groups or communities where the density of those nodes within the group is greater than that of nodes outside the group. As a result, communities of individuals are identified where the members of the community are more connected to each other than any other people in the network. For example, the subset of Taimour's social network shown in Figure 3 could be identified as a group in a large social network. We see that there are several connections between the intermediaries that serve as friends of friends and Khan himself along with Taimour's connection to this group. Depending on how the parameters are set for the community detection algorithm, many different types of groups may be identified. They could identify groups of sympathizers, intermediaries, leadership, or mix of all three. Essentially any pocket of increased connectivity. When examining social networks, it is important to identify these groups because the increased connectivity between the individuals will indicate some type of coordinated activity. For example, a group of sympathizers may be communicating on social media and actively seeking information and propaganda relating to the terrorist cause. A group of intermediaries whose job it is to bridge the gap between these sympathizers and leadership may also be identified. Community detection algorithms are valuable to the examination of social networks to identify these pockets of activity in a larger network so they can be further investigated.

6 Conclusion

Given the popularity and widespread use of social media sites across the world, terrorist groups have targeted the sites as new grounds for spreading their propaganda and recruiting new members. Targeting social media sites provides terrorists groups with a number of benefits over their traditional recruiting efforts. They are able to reach many more people essentially anywhere in the world, given free web hosting to upload content, have the ability to control access, and social media pages are less prone to attack. Once the terrorists gain a foothold on social media sites, they look to build virtual online terrorists networks where influence and ideas can flow from existing members to potential recruits. They leverage friend of a friend relationships where indirect connections allow influence and propaganda to make its way from leadership and web sites to sympathizers who may be inclined

to join their cause. Although the sympathizers may not be directly connected to the main influencers, the information and ideas still flow through intermediaries to reach them. Mainly, it is the friends that sympathizers make on social media sites that are responsible for delivering the propaganda. This social phenomenon has been exhibited as extremist groups hold question and answer sessions with leadership through Facebook and use Twitter posts to keep followers updated on the latest activity. It has also shown direct results by inspiring lone wolf terrorists. Taimour al-Abdaly injured two others while blowing himself up in Stockholm. Arid Uka acted against U.S. soldiers, murdering two and injuring another two. Later research showed these individuals were heavily immersed in virtual terrorist networks. They had friends that were connected to radical terrorists and consumed anti-Western material as it made its way to them on Facebook and YouTube. By targeting this type of behavior on social media sites, social network analysis can be used to identify these relationships. Using techniques such as ego network analysis, betweenness centrality, and community detection algorithms, the sympathizers, intermediaries, and leadership that constitute these friend of a friend relationships can be identified. Locating these relationships is extremely important so actions can be taken to disrupt the flow of influence and propaganda and prevent the existing terrorist groups from inspiring lone wolf terrorists.

7 References

- [1] al-Shishani, M. B. (2010, February 4). *Taking al-Qaeda's Jihad to Facebook*. Retrieved from The Jamestown Foundation: [http://www.jamestown.org/single/?no_cache=1&tx_ttnews\[tt_news\]=36002](http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=36002)
- [2] Witte, G., Markon, J., & Hussain, S. (2009, December 13). *Pakistani authorities hunt for alleged mastermind in plot to send N. Virginia men to Afghanistan to fight U.S. troops*. Retrieved from The Washington Post: <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/12/AR2009121201598.html?sid=ST2009121002234>
- [3] Reeder, D. (2011, June 27). *Jihadi Social Media*. Retrieved from DefenseTech: <http://defensetech.org/2011/06/27/jihadi-social-media/>
- [4] Stalinsky, S. (2011, October 7). *Why Haven't The Taliban's Twitter Accounts Been Shut Down?* Retrieved from The Middle East Media Research Institute: <http://www.memri.org/report/en/0/0/0/0/0/5707.htm>
- [5] Bumgarner, J., & Mylrea, M. (2010, March 23). *Jihad in cyberspace*. Retrieved from PoliceOne: <http://www.policeone.com/communications/articles/2025862-Jihad-in-cyberspace/>
- [6] Bardin, J. (2010). *Cyber Jihadist Use of the Internet: What Can Be Done?* Retrieved from Treadstone 71: <http://treadstone71.com/whitepapers/CyberJihadistUseoftheInternet.pdf>
- [7] Holtmann, P. (2011, March). *No threat at first sight: Invisible terrorist environments on Facebook and Youtube*. Retrieved from University of Vienna: <http://www.univie.ac.at/jihadism/blog/wp-content/uploads/2011/03/Philipp-Holtmann-No-threat-at-first-sight-Invisible-terrorist-environments-on-Facebook-and-Youtube.pdf>
- [8] Green, R. (2010, December 13). *Social Network Jihad Part 1*. Retrieved from The Middle East Media Research Institute: <http://www.memri.org/report/en/0/0/0/0/0/4834.htm>
- [9] *Social Jihad Network : Taliban Twitter*. (2011, February 21). Retrieved from SITE Intel Group: <http://news.siteintelgroup.com/component/content/article/438-taliban-twitter>
- [10] *Taimour al-Abdaly AKA Taimour Abdul Wahab*. (2010, December 13). Retrieved from Internet Haganah: <http://internet-haganah.com/harchives/007103.html>
- [11] *Two degrees from a suicide bomber*. (2011, February 25). Retrieved from Internet Haganah: <http://internet-haganah.com/harchives/007175.html>
- [12] *The Frankfurt shooter's Facebook page, and a little color commentary*. (2011, March 3). Retrieved from Internet Haganah: <http://internet-haganah.com/harchives/007191.html>
- [13] *That network diagram [Taimour al-Abdaly, Salahudin Ibn Ja'far, and Samir Khan]*. (2011, January 7). Retrieved from Internet Haganah: <http://internet-haganah.com/harchives/007132.html>
- [14] *Azeri Jihad Media and the Frankfurt shooting*. (2011, March 7). Retrieved from Internet Haganah: <http://internet-haganah.com/harchives/007198.html>
- [15] Klausen J., Barbieri, E.T., Reichlin-Melnick, A., & Zelin, A.Y. (2012). *The YouTube Jihadists: A Social Network Analysis of Al-Muhajiroun's Propaganda Campaign*. Retrieved from Perspectives on Terrorism: <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/klausen-et-al-youtube-jihadists/html>
- [16] Hanneman, R.A., & Riddle, M. (nd). *Chapter 9: Ego networks*. Retrieved from Robert Hanneman's Homepage: http://faculty.ucr.edu/~hanneman/nettext/C9_Ego_networks.html