UNDERSTANDING STRATEGIC INFORMATION MANOEUVRES IN NETWORK MEDIA TO ADVANCE CYBER OPERATIONS: A CASE STUDY ANALYSING PRO-RUSSIAN SEPARATISTS' CYBER INFORMATION OPERATIONS IN CRIMEAN WATER CRISIS

Samer AL-KHATEEB and Nitin AGARWAL†
†Maulden-Entergy Chair Professor of Information Science
University of Arkansas at Little Rock

ABSTRACT The inexpensive nature and wide availability of emerging media outlets, e.g. social networking sites and blogs makes them easy-to-use weapons, giving power and courage to individuals to form groups that are able to win or at least force concessions from stronger forces. Today, terrorist groups know that opinions can be influenced using networked media and this knowledge empowers and enables them to alienate their audience and sometimes provoke them into violent actions. To understand the strategic information manoeuvres used by such groups, e.g., trans-national terrorist groups, we study the channels (blogs, Twitter, etc.) and methods (e.g., influential actors/groups) they use to disseminate messages pertaining to recruitment, radicalization, and raising funds. We collect data from several sources, including over 130 blog websites known for pro-Russian propaganda for events such as the Crimean water crisis and Trident Juncture Exercise (TRJE 15). In addition to blogs, we collect data from Twitter for the above-mentioned events to study the cross-influence of various social media platforms in conducting strategic information manoeuvres. The study shows that groups are able to

spread their opinions and create emotional attitudes for their followers through the sophisticated and blended use of these network media platforms via powerful actors, trolls, and botnets. We design social and network science informed methodologies to study the sociotechnical behaviours of trolls and botnets and develop detection tools ready to be deployed for Cyber operations. The tools have been further tested in the information operations of ISIL, e.g., beheading of hostages in orange jump suits. This study helps identifying the actions needed to win this "battle of ideas".

Introduction

The Internet is indisputably one of the greatest inventions of the 21st century that has revolutionized communication and information dissemination. Its affordability and ease of use has made a tremendous contribution to human life in various aspects, such as education, healthcare, and business among others. People nowadays can attend colleges online, check how many calories they consumed or burned using various mobile apps, and business owners can keep track of their stocks and the progress of their company. However, with all these benefits of the Internet technologies, there are also some adverse effects.

Since the Internet provides global connectivity some individuals have abused the power of the Internet as a weapon or a tool to force concessions from stronger forces. For the last one and a half decades the Internet and specifically social media has become an integral part of conflict environments due to the democratization of technology (Tatham et al., 2008). Social media and digital communication tools have largely been considered as positive vehicles of change. However, the power of social media has been harnessed by extremists and terrorist groups to spread propaganda and influence mass thinking. As our government and corporations begin to rely more and more on social media and online

crowdsourcing for situational awareness and data, they will need to be able to identify, track in real time, and mitigate the risks. Existing approaches to cyber threat assessment and mitigation strategies overlook the societal aspect, which warrants the need for novel socio-computational methods.

The role of network media during the uprising of crises and conflicts is observed heavily (Nissen, 2015; Tatham et al., 2008). Many organizations around the world hire people, pay a lot of money, and use different techniques to spread a message or propaganda in an attempt to influence public opinion in their favour. They use different methods (bots and/or trolls) and spread misinformation in many cases to accomplish their goal (Sindelar, 2014). Digital communication tools could pose a dangerous force against democracy as well as diplomacy. Several journalistic accounts provide empirical evidence regarding strategic and tactical manoeuvre of information using social media to exploit local grievances, steer mass thinking, polarize communities, and mobilize crowds. In the Ukraine-Russia crisis, sites like ВКонтакте (VKontakte – a Russian social media platform), LiveJournal, and other blogging platforms (e.g., Tumblr, etc.) have been used as propaganda machines to justify the Kremlin's policies and actions (Allen, 2014; Bohlen, 2014). According to Interpret Magazine, the Kremlin recruited over 250 trolls, each being paid $917 per month to work round the clock to produce posts on social media and mainstream media. These trolls would manage a stream of invective against unflattering Western articles about Russia and pro-Ukrainian media by posting several comments and blog posts a day using multiple 'sock puppet' accounts. Such *troll armies* (or more commonly known as 'web brigades') piggyback on the popularity of social media to disseminate fake pictures and videos and coordinate some of the very effective disinformation campaigns, to which even legitimate news organizations could fall prey. To stem the tide of fakery or at least make the people aware,

online crowdsourcing-based efforts like StopFake.org have been created to identify and debunk fake imagery and stories about the war in Ukraine. However, such efforts are severely limited and easily outnumbered by the vast troll armies.

A similar trend has been observed in the online activities of the Islamic State terrorist organization, also known as the ISIS or ISIL. Reports have indicated that a social/collaborative answering website known as Ask.fm has been strategically used by ISIS and other extremist groups to answer questions from potential recruits (Hall, 2014). According to a report by the International Centre for the Study of Radicalization and Political Violence (ICSR), extremist organizations such as ISIS, use highly sophisticated and carefully blended social media outreach strategies (Carter et al., 2014). In fact, ISIS has developed its own Twitter app available on major platforms including Android and iOS, which is used to recruit, radicalize, and raise funds (Berger, 2014).

A recent study published by the Proceedings of the National Academy of Science of the United States of America (PNAS) coined the term "femtorisk" to refer to a statistically small phenomenon that is capable of exerting a huge impact on global politics such as the Arab Spring, the 2008 financial crisis, and Ukraine's Euromaidan protests (Berger, 2015). Although several attempts have been made to identify and study these "femtorisk" phenomena, there is still a lack of understanding in how these organizations or groups use the network media to spread their messages. This will enable authorities to take the necessary actions against these "femtorisk" phenomena.

Recently, a sharp increase in the deviant behaviours organized and conducted via the Internet has been reported, including various incidents of cybercrimes (Dye and Finkle, 2013), cyber warfare (Hoke and Babb, 2015), "Remote warfare" or "Social warfare" (Nissen, 2015), etc. Network media nowadays is also used for

military activities such as Offensive and Defensive Cyber-Operations, Intelligence Collection, Command and Control activities, Targeting, and Psychological Warfare (Nissen, 2015). All these applications where network media worked as an effective tool gave it an importance big enough to merit its study.

In this study we focus on studying how information manoeuvres are executed in network media i.e. Twitter and the likes, during the Crimean water crisis (BBC, 2014). We collect data during the crisis and analyse it in an attempt to understand the strategic information (or disinformation) dissemination campaigns conducted by groups of individuals (or trolls) and/or bots, and identify the channels (e.g., Twitter) and methods (e.g., influential actors/groups) used. Through this study we try to find answers for the following research questions:

1. How is propaganda disseminated via networked media during conflicts or crises? What roles do bots play in such information manoeuvres?

2. Can we develop a methodology to detect bot activities? We present a methodology to demonstrate bot activities in disseminating propaganda during the Crimean water crisis.

3. Is there an organizational structure to the bot activities? More specifically, who is responsible for feeding information (or rather misinformation) to these bots? What strategies do the bots use to further disseminate propaganda? And most importantly, are these bots working in collusion? Further, can we identify the positions or roles various bots assume in the networked media to effectively and efficiently coordinate the propaganda dissemination process?

Toward this direction, we make the following contributions:

- We shed light on a phenomenon that is commonly used to disseminate propaganda on networked media.

- We document coordination strategies among bots to enhance the reachability of their postings disseminating propaganda.

- An organizational structure is identified among the bots, where a real-person feeds the misinformation to a network of bots, or botnet.

- We identify network structures among bots corresponding to collective sociotechnical behaviours exhibited by a collection of bots (or, brokers) to disseminate propaganda.

- The findings will inform development of predictive models and eventually tools that can assist decision-making bodies to take necessary actions.

While some of the above mentioned contributions are specific to the Crimean water crisis case study, the findings and especially the methodology to identify bot behaviours would most certainly inform development of predictive models and eventually tools that can assist decision-making bodies to design cyber-warfare operations. The rest of the article is organized as follows. Section 2 provides an overview of bots in information operations through empirical observations and trends on some of the work done with regards to identifying bots and sociotechnical behaviours of trolls on network media. Next in Section 3, we give a brief description of the data we collected. Then we present our analysis and findings in section 4. We summarize the conclusions with implications of the research and future directions in Section 5.

Overview of Bots in Information Operations: Empirical Observations and Trends

In this study, we find out that a group of bots managed by group of brokers are disseminating information that is related and not related to the Crimean water crisis and this information was taken from a "real person" user account (the most influential node in the network). The reason was to spread propaganda about the crisis and try to grab the attention of as many people as possible. The bot activity in this network used a strategy called "*misdirection*" (a technique used by magicians to make the crowd look somewhere else while they are performing the trick. For example, the bot would tweet unrelated news that is happening somewhere else but still mention a hashtag related to the Russia-Ukraine water crisis) and "*smoke screening*" (when a bot would mention something about Russia or Ukraine but not necessary related to the water crisis). Similar techniques have been used in the Syrian Social Bot (SSB) to raise awareness of the Syrian civil war (Abokhodair et al., 2015 pp. 839–851).

Automated Social Actors/Agents (ASAs) or bots or botnets (a network of bots colluding with each other) are not a new phenomenon and they have been studied in the literature previously in a variety of domains. One of the earliest studies focused on the usage of social bots that were used in the Internet Relay Chat (IRC), such as Eggdrop, which emerged in early 1993 (Rodríguez-Gómez et al., 2013). This bot's tasks were welcoming and greeting new participants and also warn users about other users' actions. The usage of bots on IRC was very popular due to the simplicity to implement it and its ability of scaling IRC (Karasaridis et al., 2007).

As time progressed, social bots got more sophisticated and have more advanced functionality. Another study in this direction is the study of social bots usage on Multi-User-Domains (MUDs) and

Massive Multiplayer Online Games (MMOGs). The emergence of Multi User Domains calls for the need for automated social actors (ASAs) to enhance the playing experience. As the online gaming market grew, the call for more advanced bots increased. In MMOGs, such as the World of Warcraft (WoW) unauthorized game bots emerged. These unauthorized bots enhance and trigger mechanisms for the players by often sitting between the players' client application and the game server. Some of these bots were also able to play the game autonomously in the absence of the real player. In addition to that, some bots were also able to damage the game ecologies, i.e., amassing experience points or game currency (virtual gold, etc.). (Abokhodair et al., 2015 pp. 839–851).

As social media emerged, the usage of social botnets sparked. A study conducted in 2012 by Facebook estimated that roughly 5-6% of all Facebook users are fake accounts. This means that there are a large number of user accounts that do not represent real people (about 50 million users). So the natural question is, who owns these accounts? (Protalinski, 2012). One study focused on how vulnerable Facebook is to these bots and how these bots are thriving to mimic human behaviour so they would be hard to detect/capture (Boshmaf et al., 2012 p.12). A similar study to ours was conducted on the Syrian civil war conflict by Abokhodair et al. (2015, pp. 839–851), who focused on one bot that lived for six months before Twitter detected it and suspended it. The study analysed the life and the activities of that bot. More focus was given on the content of the tweets, i.e., categorizing the tweets into news, opinion, etc. The difference between their study and ours is, we are focusing on identifying the network structure of a group of bots, which are managed by a real person node (to find the leader or the most influential node in the network). To the best of our knowledge it is the first attempt to identify a bot network structure or a botnet, during crises and detect their communication and information dissemination strategies. Further, we identify the roles

and positions assumed by the bots within their group (such as brokers who serve as bridges between different parts of the network or sub networks) for affecting various information manoeuvres.

Research Methodology

In this study, we take the Crimean water crisis as a case to study. During the time of crisis there was an article published by the BBC news (BBC, 2014) with the title "Russia fears Crimea water shortage as supply drops". In this article, the BBC was reporting about the Russian officials who told BBC that a water shortage in Crimea is threatening to become acute because Ukraine has reduced the supply via a key canal. The dissemination of this news article was very intense in social media, especially Twitter. Usually Twitter is the "go to" medium for propaganda dissemination because it is easy to use, a mass dissemination platform (a message can reach millions of users in a short period of time), and hyper connected (a user can have thousands or even millions of friends/followers who are highly interconnected). Also, because of Twitter's operational capabilities tricks like "thread-jacking" (the change of topic in a "thread" of discussion in an open forum) and "hashtag-latching" (strategically associating unrelated but popular or trending hashtags to target a broader, or in some cases a very specific audience) are prevalent and easily done. In addition to Twitter other tools that can be used include blogs, YouTube, Facebook, for Russian cyber operations, ВКонтакте. Such tools are gaining popularity among the cyber trolls/agents. During the aforementioned water crisis many bots were tweeting the same article using a link to a website that copied the original BBC article and made it look like it was published by itself. We use this case to examine how propaganda is spread with the help of bots on social media channels during the troubling and chaotic times of crises.

The findings in this study can be further examined in other crises in future. By studying as many crises as possible behavioural patterns would start to emerge, which can then help build tools to understand narratives and help shape counter-narratives during the time of crises. To study the strategic information manoeuvres on network media we have collected data during the Crimean water crisis. A brief description of the dataset and our findings are presented next.

Data Collection

We have used TweetTracker (Kumar et al., 2011), and NodeXL (Smith et al., 2009 pp. 255–264) tools to collect data for the period between 4/29/2014 8:40:32 PM and 7/21/2014 10:40:06 PM UTC. This resulted in 1,361 tweets, 588 Twitter users, and 118,601 relations between the Twitter users. There are four basic types of relations in the Twitter data, viz., *follows*, *mentions*, *replies*, and *tweets*. A snapshot of a tiny sample of tweets is depicted below (see figure 1). Each tweet is wrapped around by unrelated hashtags, mainly the name of cities, states, or countries. The tweets are identical, and include a hyperlink to the same article, which contains the propaganda message that the bots are employed to disseminate.

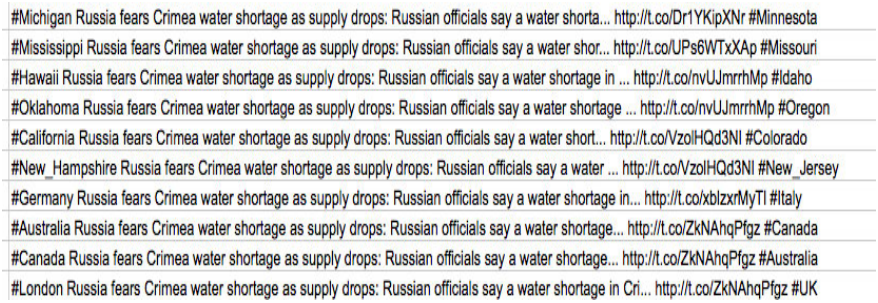

Figure 1. A snapshot for a sample of the tweets collected during the Crimean water crisis

Analysis, Results & Findings

By analysing the tweets and their content we observed a few anomalous behaviours, such as:

1. Many tweets are identical, i.e., different Twitter users posted the same tweets. Note that these are not retweets.

2. The frequency of the tweets was unusually high, i.e., a large number of tweets were posted in a very short duration – a behaviour that is humanly impossible.

3. All tweets contain 'short' links, pointing to the same article on a specific website.

4. All the tweets are bracketed within a pair of hashtags, i.e., there is a beginning and an end hashtag for every tweet.

5. These hashtags are not related to the tweet content. This indicates the presence of "misdirection" and "smoke screening" (Abokhodair et al., 2015 pp. 839–851) strategies. More specifically, the hashtags correspond to the names of cities, states, and countries of the world, completely unrelated to the content of the tweet as well as the webpage pointed to by the short link.

6. Extremely precise repetitive patterns and correlations were observed, e.g., users with Arabic names did not provide location information and users with non-Arabic names provided locations in the Arab/Middle-East regions.

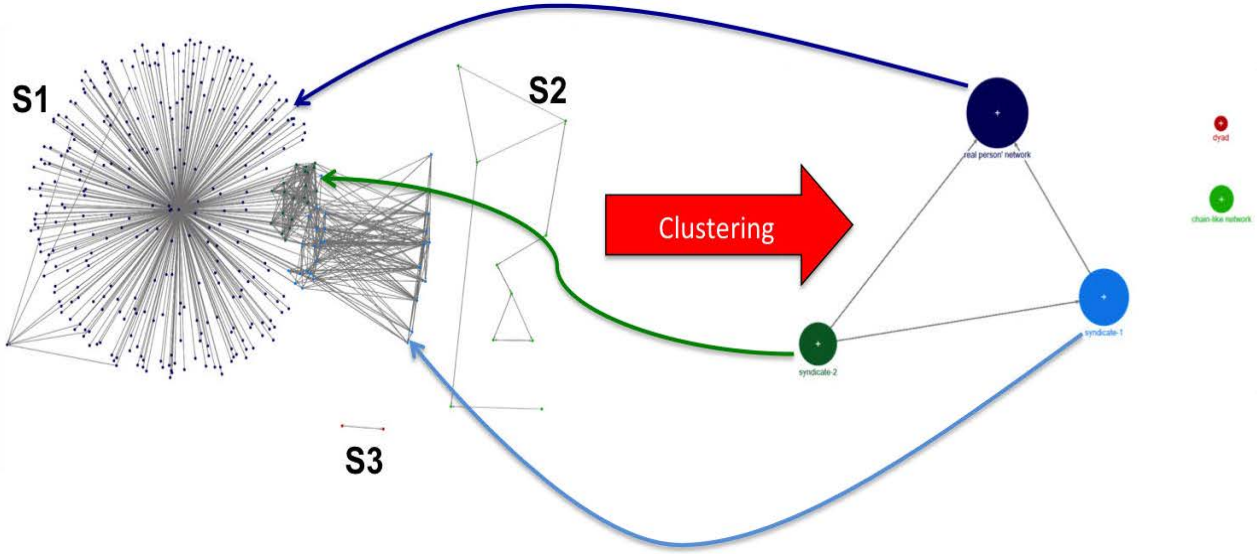

Figure 2. Three sub-networks with unusual structural characteristics in S1 are observed, Girvan-Newman clustering algorithm is applied to the network. On the left are the expanded clusters and on the right is the collapsed view of the clusters. Five clusters are identified.

Such an anomalous behaviour is characteristic of computer software, or a bot that can autonomously operate Twitter. Further analysis is conducted to investigate whether these bots are connected and if they are coordinating. To identify the relationships between these twitter users, we collected their friends and followers network. This resulted in 1,584 edges among the 588 unique Twitter users. The network is presented in figure 2.

By examining the visualized network we find out that this network has three sub-networks S1, S2, and S3. The sub-network S1 exhibits unusual structural characteristics so we zoom in on it. The other two sub-networks (the 'dyadic' S3 and the 'chain-like' S2 sub-networks) were ignored due to their relatively small size and lack of any anomalous behaviour. We applied the Girvan-Newman clustering algorithm (Girvan and Newman, 2002 pp. 7821–7826) to this network and we found out that the network has five clusters as shown in figure 2. By diving into the analysis of S1 we find out it has a star shaped and two clique-style groups of nodes. The centre of the star-shaped network belongs to a "real person" node, which is connected to 345 bots out of 588 twitter handles in this network. This person is the owner/operator of the specific webpage that all the other bots were referring to with different shortened links. Next, we un-collapse one group at a time and examine its group-level coordination network:

- Un-collapsing the "real person" network (figure 3a) reveals its star-shaped structure, where the "real person" is the central node. It also shows the connections to the other two-syndicate groups, viz., syndicate-1 and syndicate-2. Closely examining these ties reveals that the members of the syndicate follow the "real person" node and not the other way. We can thus conclude that the "real person" is the most central node of this entire bot network and is the one who feeds information to the bots.

- Un-collapsing the syndicate-1 network (figure 3b) reveals dense connections among its members and inter-group connections with the other groups, viz., the "real person" network and 'syndicate-2'. Closer examination of the within group ties, reveals a mutually reciprocated relationship, suggesting the principles of 'Follow Me and I Follow You' (FMIFY) and 'I Follow You, Follow Me' (IFYFM) in practice - a well-known practice by Twitter spammers for link farming or quickly gaining followers (Ghosh et al., 2012 pp. 61–70)(Labatut et al., 2014 p. 8). Unlike the "real person" network, there is no single most central node in this network, indicating an absence of a hierarchical organization structure in the 'syndicate-1' network.

- Un-collapsing the syndicate-2 network (figure 3c) reveals dense connections among its members and inter-group connections with the other groups, viz., the "real person" network and 'syndicate-1'. Closer examination of the within group ties, reveals a mutually reciprocated relationship, suggesting the principles of 'Follow Me and I Follow You' (FMIFY) and 'I Follow You, Follow Me' (IFYFM) in practice - a well-known practice by Twitter spammers for link farming or quickly gaining followers (Ghosh et al., 2012 pp. 61–70) (Labatut et al., 2014 p. 8). Unlike the "real person" network, there is no single most central node in this network, indicating an absence of a hierarchical organization structure in 'syndicate-2' network.

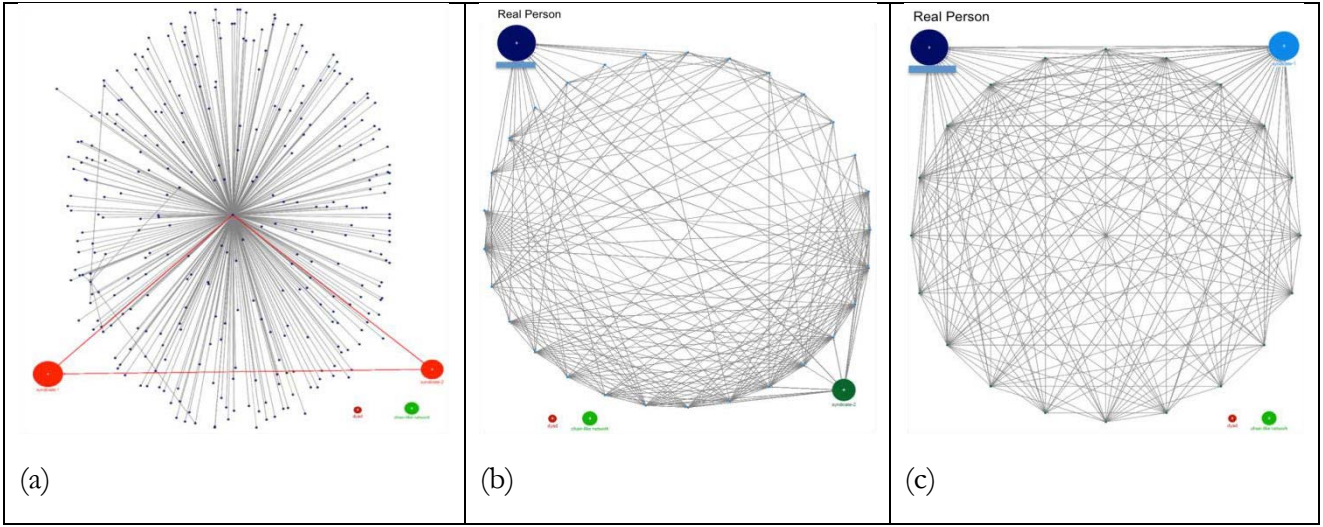

Figure 3. (a) Un-Collapsing "Real Person" Network. (b) Un-Collapsing Syndicate 1 Network. (c) Un-Collapsing Syndicate 2 Network.

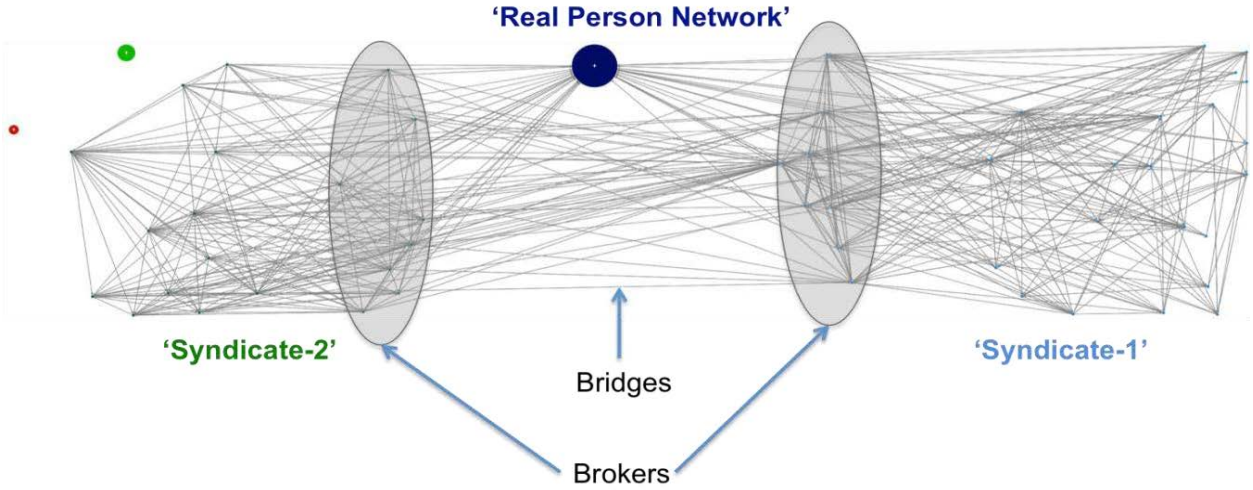

Figure 4. The real person network is connected to the brokers who coordinate the dissemination of propaganda through the bots in their respective syndicates.

Further analysis showed that the broker nodes act as interfaces between the group members and other groups. The broker nodes of the two syndicates establish bridges that facilitate tweet exchange across the syndicates. Broker nodes are also primarily responsible in connecting with the 'real person network', specifically the 'real person' node (the most influential node). This indicates a highly sophisticated coordination in this bot network as can be seen in figure 4.

The analysis helps in answering our research questions stated earlier. More specifically:

Research Question 1: How is propaganda disseminated via networked media during conflicts or crises? What roles do bots play in such information manoeuvres?

Discussion: Propaganda is disseminated via social media sites especially Twitter and blog sites during crises for the aforementioned reasons. Botnets act as mass dissemination tools used by individuals or groups to spread their agenda and influence mass thinking or misinformation about specific events. These bots are getting more sophisticated and use many techniques such as "misdirection" or "smoke screening" to guarantee the wide visibility of their tweets contents.

Research Question 2: Can we develop a methodology to detect bot activities?

Discussion: Yes this can be done, and there are already some tools out there that can detect botnets with different accuracy, viz., Scraawl (https://www.scraawl.com). We are working toward this direction, in collaboration with the Scraawl team. We believe by studying as many crises as possible, behavioural patterns would start to emerge, which can then help build tools to understand

narratives and help shape counter-narratives during the time of crises.

Research Question 3: Is there an organizational structure to the bot activities? More specifically, who is responsible for feeding information (or rather misinformation) to these bots? What strategies do the bots use to further disseminate propaganda? And most importantly, are these bots working in collusion? Further, can we identify the positions or roles various bots assume in the networked media to effectively and efficiently coordinate the propaganda dissemination process?

Discussion: There is an organizational structure to the bot activities depicted in the Real Person Network of figure 4, especially the brokers and bridges. Usually a real person account or accounts, managed by a group of individuals, feed the propaganda to the bots then botnets take care of the rest of the job in spreading this propaganda. Bots use many strategies to spread the agenda they are assigned to disseminate such as smoke screening and misdirection. These bots are also working in collusion (working together) to disseminate the agenda. Roles and positions can also be identified such as: the real person node has a star shaped network in this case (figure 3a), brokers are the nodes that form communication or information bridges between the real person network and the botnets (can be seen in figure 4), then the botnets have a clique network (depicted in syndicate network 1 and 2, figure 3b and 3c respectively).

Implications & Future work

This study shows the strategic information manoeuvre used by groups to disseminate propaganda in and through network media, specifically Twitter. Such strategies and behaviours (misdirection and smoke screening) are worth studying as they lead to developing tools that can help understand propaganda

dissemination and shape counter-narratives enabling the authorities to take effective actions in cyber space or on the ground. Our future directions include working on developing social science and network science informed methodologies that can mine such behavioural patterns on network media. We are testing these methodologies on datasets collected during the propaganda dissemination (via tweets, blogs, etc.) containing videos, images, and other memes (e.g., hashtags, etc.) for beheading of hostages by the Islamic extremist terrorist groups, such as ISIL, including the beheading of Arab-Israeli 'Spy' in Syria, the beheading of Copts in Libya, and the beheading of Ethiopian Christians in Libya.

Acknowledgement

This material is based upon work supported by the U.S. Office of Naval Research under Grant No. N000141410489 and the Jerry L. Maulden/Entergy Foundation at the University of Arkansas at Little Rock. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding organization. The researchers gratefully acknowledge the support.

Bibliography

Abokhodair, N., Yoo, D., McDonald, D.W., 2015. Dissecting a Social Botnet: Growth, Content and Influence in Twitter, in: Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing. ACM.

Allen, M., 2014. Kremlin's "social media takeover": Cold War tactics fuel Ukraine crisis [WWW Document]. Democr. Dig. Natl. Endow. Democr. URL http://www.demdigest.net/blog/kremlins-social-media-takeover-cold-war-tactics-fuel-ukraine-crisis/ (accessed 5.27.15).

BBC, N., 2014. Russia fears Crimea water shortage as supply drops [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-27155885 (accessed 5.27.14).

Berger, J.M., 2015. How ISIS Succeeds on Social Media Where #StopKony Fails [WWW Document]. The Atlantic. URL http://www.theatlantic.com/international/archive/2015/03/how-isis-succeeds-where-stopkony-fails/387859/ (accessed 5.27.15).

Berger, J.M., 2014. How ISIS Games Twitter: The militant group that conquered northern Iraq is deploying a sophisticated social-media strategy [WWW Document]. The Atlantic. URL http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/ (accessed 5.27.15).

Bohlen, C., 2014. Cold War Media Tactics Fuel Ukraine Crisis [WWW Document]. The Times. URL http://www.nytimes.com/2014/03/11/world/europe/cold-war-media-tactics-fuel-ukraine-crisis.html (accessed 5.27.15).

Boshmaf, Y., Muslukhov, I., Beznosov, K., Ripeanu, M., 2012. Key challenges in defending against malicious socialbots, in: Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats. USENIX Association.

Carter, J.A., Maher, S., Neumann, P.R., 2014. #Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks. The International Center for the Study of Radicalization and Political Violence (ICSR).

Dye, J., Finkle, J., 2013. US Charges Eight in $45 Million Cybercrime Scheme [WWW Document]. CNBC. URL http://www.cnbc.com/id/100724220#. (accessed 5.6.15).

Ghosh, S., Viswanath, B., Kooti, F., Sharma, N.K., Korlam, G., Benevenuto, F., Ganguly, N., Gummadi, K.P., 2012. Understanding and combating link farming in the twitter social network, in: Proceedings of the 21st International Conference on World Wide Web. ACM.

Girvan, M., Newman, M.E.J., 2002. Community structure in social and biological networks. Proc. Natl. Acad. Sci. U. S. Am. 99. doi:10.1073/pnas.122653799

Hall, J., 2014. "U dont need much, u get wages here, u get food provided and place to stay": The rough travel guide British ISIS fighters are using to lure fellow Britons in to waging Jihad in Iraq. [WWW Document]. Dly. Mail. URL http://www.dailymail.co.uk/news/article-2661177/Travel-light-leave-Islamic-books-home-dont-arouse-suspicion-Isis-militants-offer-travel-advice-jihadists-arriving-Syria-Iraq-Britain.html (accessed 5.27.15).

Hoke, Z., Babb, C., 2015. FBI Investigating Cyber Attack on US Central Command. Voice Am. URL http://www.voanews.com/content/us-centcom-twitter-hacked-apparently-by-is-group/2595139.html (accessed 5.6.15).

Karasaridis, A., Rexroad, B., Hoeflin, D., 2007. Wide-scale botnet detection and characterization, in: Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets. Cambridge, MA.

Kumar, S., Barbier, G., Abbasi, M.A., Liu, H., 2011. TweetTracker: An Analysis Tool for Humanitarian and Disaster Relief., in: ICWSM.

Labatut, V., Dugue, N., Perez, A., 2014. Identifying the Community Roles of Social Capitalists in the Twitter Network. Presented at the IEEE/ACM International Conference on

Advances in Social Network Analysis and Mining (ASONAM), China. doi:10.1109/ASONAM.2014.6921612

Nissen, T.E., 2015. #TheWeaponizationOfSocialMedia.

Protalinski, E., 2012. Facebook: 5-6% of accounts are fake [WWW Document]. ZDNet. URL http://www.zdnet.com/article/facebook-5-6-of-accounts-are-fake/ (accessed 5.8.15).

Rodríguez-Gómez, R.A., Maciá-Fernández, G., García-Teodoro, P., 2013. Survey and taxonomy of botnet research through life-cycle. ACM Comput. Surv. CSUR 45, 45.

Sindelar, D., 2014. The Kremlin's Troll Army [WWW Document]. TheAtlantic. URL http://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/ (accessed 5.6.15).

Smith, M.A., Shneiderman, B., Milic-Frayling, N., Mendes Rodrigues, E., Barash, V., Dunne, C., Capone, T., Perer, A., Gleave, E., 2009. Analyzing (social media) networks with NodeXL, in: Proceedings of the Fourth International Conference on Communities and Technologies. ACM.

Tatham, S.A., Defence Academy of the United Kingdom, Advanced Research and Assessment Group, 2008. Strategic communication: a primer. Defence Academy of the United Kingdom, Advanced Research and Assessment Group, Shrivenham.