Social Cyber Forensics Approach to Study Twitter's and Blogs' Influence on Propaganda Campaigns

Samer Al-khateeb, Muhammad Nihal Hussain, and Nitin Agarwal

Department of Information Science
University of Arkansas at Little Rock
Little Rock AR 72204, USA

{sxalkhateeb,mnhussain,nxagarwal}@ualr.edu

Abstract: In today's information technology age our political discourse is shrinking to fit our smartphone screens. Online Deviant Groups (ODGs) use social media to coordinate cyber propaganda campaigns to achieve strategic and political goals, influence mass thinking, and steer behaviors. In this research, we study the ODGs who conducted cyber propaganda campaigns against NATO's Trident Juncture Exercise 2015 (TRJE 2015) and how they used Twitter and blogs to drive the campaigns. Using a blended Social Network Analysis (SNA) and Social Cyber Forensics (SCF) approaches, "anti-NATO" narratives were identified on blogs. The narratives intensified as the TRJE 2015 approached. The most influential narrative identified by the proposed methodology called for civil disobedience and direct actions against TRJE 2015 specifically and NATO in general. We use SCF analysis to extract metadata associated with propaganda-riddled websites. The metadata helps in the collection of social and communication network information. By applying SNA on the data, we identify influential users and powerful groups (or, focal structures) coordinating the propaganda campaigns. Data for this research (including blogs and metadata) is accessible through our in-house developed Blogtrackers tool.

Keywords: cyber propaganda campaign, misinformation, NATO, Trident Juncture Exercise, narrative, influence, blogs, Twitter, social media, social network analysis, cyber forensics, Blogtrackers, social cyber forensics.

1 Introduction

The inexpensive nature, ease of use, and the popularity of social media makes it a powerful tool that can be used to disseminate misinformation or coordinate cyber propaganda campaigns in order to influence mass thinking and steer behaviors or perspectives about an event. We investigate these phenomena in this research. Social media provides a rich source of information [1]. With millions of social network users around the globe, cyber forensic analysis of social media has profound applications [2]. Cyber forensic analysis of social media can help collect evidence that helps investigators develop a strong case [1]. Cyber Forensics (CF) is "the process of acquisition, authentication, analysis, and documentation of evidence extracted from and/or contained in a computer system, computer network, and digital media" [3]. With the use of metadata, extracted using cyber forensics the relationship between deviant groups can be discovered. In this work, we identify and study the behavior of these ODGs and how they use social media to coordinate cyber propaganda campaigns using SNA and SCF techniques. We define ODGs as a collective that organizes a harmful activity using cyber space in which its result would affect cyber space, physical space or both, i.e., the "Cybernetic Space" [4]. We also develop methodologies to identify influential narratives in a cyber campaign. We use Maltego (available at: http://bit.ly/1Vm00JS) to conduct SCF analysis and enhance the collected data. We use SNA in combination with the metadata extracted from SCF analysis to have a comprehensive understanding of the propaganda campaign coordination. For conducting SNA we use NodeXL (available at: https://nodexl.codeplex.com) and Focal Structure Analysis (FSA) (available at: www.merjek.com). FSA helps discover an influential group of individuals in a large network. These individuals are connected and may not be the most influential individually, but by acting together they form a compelling power. We chose this approach because it was tested on many real world events including the Saudi Arabian women's right to drive campaign on Twitter (Oct26Driving), and the 2014 Ukraine Crisis when President Viktor Yanukovych rejected a deal for greater integration with the European Union [5]. For analyzing blog data, we use Blogtrackers (available at: http://blogtrackers.host.ualr.edu/).

This research has implications not only to the scientific community, but also for authorities as these ODGs pose non-negligible concerns for public safety and national security, e.g., one of the influential narratives in the data collected in this study called for civil disobedience, planned protests, or direct actions against the TRJE 2015 exercise. Therefore, we study: (1) Who are the important information actors in the campaign network? (2) What is the role of each social media channel in the propaganda campaign coordination? (3) What is the public opinion mostly concerned about? (4) Who are the coordinating network structure and influential groups (or, ODGs) in the campaign network, or in other words which set of nodes are most powerful in disseminating the message? (5) Can we identify influential narratives in the cyber campaign?

2 Literature Review

Digital forensics tools have been mainly used by law enforcement agencies for detecting and solving corporate fraud [6]. Cyber forensics tools can be traced back to the early 1980's when these tools were mainly used by government agencies, e.g., the Royal Canadian Mounted Police (RCMP) and the U.S Internal Revenue Service (IRS). With time, these tools got more sophisticated and in the mid of 1980's these tools were able to recognize file types as well as retrieve lost or deleted files, e.g., *XtreeGold* and *DiskEdit* by Norton. In 1990's these tools became more popular with more capabilities, e.g., recovering deleted files and fragments of deleted files using *Expert Witness* and Encase [7]. Nowadays, many tools are available to public to collect cyber forensics data and visualize it, e.g., Maltego. Blogs provide rich medium for individuals to frame an agenda and develop a discourse that could possibly influence the masses. Twitter, however due to the 140-character limit is primarily used as a dissemination medium. Typically, bloggers use Twitter to build an audience and as a vehicle to carry their message to their audience. It is important to understand the disinformation dissemination network on Twitter but it is equally, if not more, important to understand the blog environment and specifically the blogger's influence, engagement with the audience, and motivations for agenda setting. Identifying influential individuals in blogosphere is a well-studied problem. Many studies have been conducted to identify influence of a blogger in a community [8]. A blog post having more in-links and comments indicates that the community is interested in it.

3 Methodology

The overall methodology of this study is depicted in **Fig. 1**. We identified six groups by searching their names on various social media platforms to identify their Twitter and blogging profiles. NATO's public affairs officers then verified these profiles. These six groups propagate their messages on social media inviting people to act against NATO and TRJE 2015 exercise. An initial set of twelve blog sites were identified that the groups use to develop narratives against the TRJE 2015 exercise. We were also able to identify Twitter handles used to steer the audience from Twitter to their blogs. We identified an initial set of 9 Twitter accounts used by the six groups. We used Twitter API through a tool called *NodeXL* to collect a network of *replies, mentions, tweets, friends*, and *followers* for all the nine Twitter accounts and whoever is connected to them with any one of the aforementioned relationships for the period 8/3/2014 to 9/12/2015. The dataset file we obtained contains 10,805 friends/followers, 68 replies, 654 tweets, 1,365 mentions, 9,129 total nodes, and 10,824 total edges. The twitter handles, blogs, and names of the groups studied in this research are publically available. However, in order to ensure their privacy, we do not disclose them here.

Metadata Extraction Using Maltego: Maltego is an open source information gathering and forensics application. Maltego can extract Google Analytics IDs from blog sites. Google Analytics is an online analytics service that allows a website owner to gather statistics about their website visitors such as their browser, operating system, and country among other metadata. Multiple sites can be managed under a single Google analytics account. The account has a unique identifying "UA" number, which is usually embedded in the website's html code [9]. Using this identifier other blog sites that are managed under the same UA number can be identified. This method was reported in [9] [10]. So by using Maltego we can infer connections among blog sites and identify new sites that were previously undiscovered.

We used a seed set of 12 blog sites to discover other blogs that are connected to them using Maltego as explained earlier. We used Maltego in a snowball manner to discover other blog sites. We were able to identify additional 9 blogs that are connected to the initial seed blogs by the same Google analytics IDs. These newly identified websites have the same content published on different portals and sometimes in dif

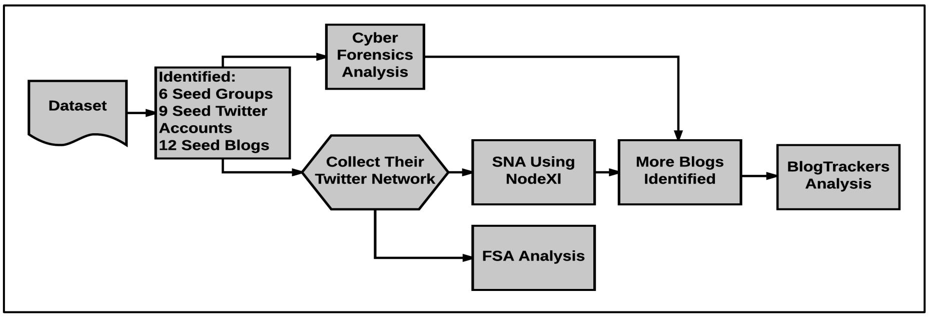

Fig. 1. Proposed methodology to analyze propaganda campaigns.

ferent languages. For example, a website written in English may also have another identical version but written in another language that is native to the region. Such blogs are also known as *bridge blogs* [11]. We went a step further to collect the IP addresses, website owner name, email address, phone numbers, and locations of all the websites. We obtained three clusters of websites based on their geolocation. These clusters are helpful to know the originality of the blog sites, which would help an analyst understand the propaganda that is being pushed by the specific blog site. Cluster 1 contains one website that is located in Russia, Cluster 2 has 8 websites located in USA, and Cluster 3 has 12 blog sites located in Spain, Cayman Islands, UK, and Germany. From initial 12 blog sites we grew to 21 blog sites, 6 locations, and 15 IP addresses. All the blog sites we identified during this study were crawled and their data was stored in a database that the Blogtrackers tool can access and analyze.

Applying SNA to Identify Influential Information Actors: After using Maltego to find other related blog sites used by the group to disseminate their propaganda, we applied SNA to find the most important nodes in the network by activity type. Using NodeXL we were able to find the most used *hashtags* during the time of the exercise. This helps in targeting the same audience if counter narratives were necessary to be pushed to the same audience. In addition to that, we found the most tweeted *URLs* in the graph. This gives an idea about the public opinion concerns. And finally we found the most used *domains*, which helps to know where the focus of analysis should be directed, or what other media platforms are used. For example, two of the top 10 hashtags that were used during the TRJE 2015 exercise were #YoConvoco (that translates to “I invite” using Google translation service) and #SinMordazas (that translates to “No Gags”). These two hashtags were referring to a campaign that is asking people for protests and civil resistance or civil disobedience. Also, investigating the top 10 URLs that were shared the most in the dataset reveals that these URLs were links to websites that are mobilizing people to raise objections on using taxpayers’ money to fund military spending on wars.

Applying FSA to Identify Powerful Groups of Individuals Effecting Cyber Propaganda Campaign: We divided our network (9,129 nodes and 10,824 unique edges) into two types namely, *the social network*, derived from friends and follower’s relations and *the communication network*, derived from replies and mentions relations. We ran the FSA algorithm on these two networks to discover the *most influential* *group of nodes*. Running FSA on the *social network* resulted in 1 focal structure with 7 nodes. These 7 nodes are in fact among the nine anti-NATO seed nodes we started with and are very tightly knit (i.e., they exert mutually reciprocative relationships). This indicates a strong coordination structure among these 7 nodes, which is critical for conducting information campaigns. Running FSA on the *communication network* resulted in 3 focal structures with a total of 22 nodes. The same 7 accounts (out of the 9 seed accounts) found in the social network focal structures are distributed in these 3 focal structures. This gives those 7 accounts more power/influence than other nodes in the network because they are found in the focal structures of both networks, i.e., the communication and social network. The rest of the nodes (i.e., the additional 15 accounts) found in these 3 focal structures of the communication network are new nodes. These are important because they are either leaders or part of key groups conducting propaganda campaigns.

Using Blogtrackers to Analyze Blog Data: Using SCF analysis and SNA as explained in the previous sections, we were able to identify a total of 21 blog sites of interest. We trained web crawlers to collect data from these blogs and store the data in Blogtrackers database. We performed the following analysis: (1) we started exploring the collected dataset by generating the *traffic pattern* graph using Blogtrackers, for the period of August 2014 to December 2015. We observed a relatively higher activity in these blogs from September 2015 to December 2015, the period around the TRJE 2015, (2) then we generated a *keyword trends* graph for the keywords ‘anti nato’, ‘trident juncture’, ‘nato’. The keyword trend for the ‘anti nato’ completely aligned with the traffic pattern graph indicating the posts actually had ‘anti nato’ keyword in it. We also observed that trend for ‘anti nato’ was consistently higher than ‘nato’ for this time period indicating there was more negative sentiment towards NATO in these blogs, (3) we ran the *sentiment* analysis in Blogtrackers for the same period and observed more negative sentiment than positive sentiment in the blogs, (4) we ran the *influential posts* analysis in Blogtrackers to identify posts with high influence. In other words, we want to identify what resonates with the community most, or which narratives are affecting the people most. The most influential post was an Italian blog post from the ‘nobordersard’ blog. Upon translation to English we found the post to be highly propaganda-riddled. The blogger used two of the conventional propaganda techniques [12] called “*Name Calling*” (associating a negative word to damage the reputation) and “*Plain Folks*” (presenting themselves as ordinary people or general public to gather support for their cause or ideology). The blog post used phrases like: NATO exercise was contributing to pollution and exploiting resources. It also categorizes this exercise as an act of militarization of territories to train for war. Furthermore, the blog was asking people to protest against the exercise.

4 Conclusion, Summary, and Future Directions

In this paper, we study the ODGs and their behavior in conducting deviant acts, especially disseminating propaganda against NATO and TRJE 2015. We further study how ODGs use social media in coordinating cyber propaganda campaigns. We conducted a *node-level* analysis, a *group-level* analysis, and *content* analysis. We collected Twitter network of the six deviant groups who had 9 twitter accounts and 12 blog sites. We analyzed this network to discover who are the top users in terms of activity, i.e., tweet, retweet, or mentions. We also discovered the most used hashtags, the most tweeted URLs, and the most used domains. This served as node level analysis. Then we used SCF tool to discover other blog sites that are related to the seed blogs. This enabled us to discover how blogs are connected and if the same group owns multiple blogs. By applying FSA, we discovered the coordinating groups. This served as a *group level analysis*. We further analyzed the content of the blogs using Blogtrackers tool to discover the most prominent propaganda messages and the techniques these groups use to be effective in spreading their messages. This served as *content analysis*. The aforementioned methodologies constitute a tiny but promising sample from a spectrum of approaches to study cyber propaganda campaigns on social media.

Acknowledgements: This research is funded in part by NSF (IIS-1636933, IIS-1110868 and ACI-1429160), ONR (N000141010091, N000141410489, N0001415P1187, N000141612016, and N000141612412), AFRL, ARO (W911NF-16-1-0189), DARPA (W31P4Q-17-C-0059), and the Jerry L. Maulden/Entergy Fund at UA Little Rock.

References

[1] B. Wright, "Social Media and the Changing Role of Investigators," Forensic Mag., Dec. 2012.
[2] M. Mulazzani, M. Huber, and E. Weippl, "Social network forensics: Tapping the data pool of social networks," in Eighth Annual IFIP WG, 2012, vol. 11.
[3] D. Povar and V. K. Bhadran, "Forensic Data Carving," in Digital Forensics and Cyber Crime, vol. 53, Springer Berlin Heidelberg, 2011, pp. 137–148.
[4] S. Al-khateeb and N. Agarwal, "Analyzing Flash Mobs in Cybernetic Space and the Imminent Security Threats A Collective Action Based Theoretical Perspective on Emerg-ing Sociotechnical Behaviors," in 2015 AAAI Spring Symposium Series, 2015.
[5] F. Sen, R. Wigand, N. Agarwal, S. Yuce, and R. Kasprzyk, "Focal Structures Analysis: Identifying Influential Sets of Individuals in a Social Network," Soc. Netw. Anal. Min., vol. 6, pp. 1–22, 2016.
[6] N. Alherbawi, Z. Shukur, and R. Sulaiman, "Systematic Literature Review on Data Carving in Digital Forensic," in Procedia Technology, 2013, vol. 11, pp. 86 – 92.
[7] K. Oyeusi, "Computer Forensics," London Metropolitan University, 2009.
[8] N. Agarwal, H. Liu, L. Tang, and P. S. Yu, "Identifying the influential bloggers in a community," in Proceedings of the 2008 international conference on web search and data mining, 2008, pp. 207–218.
[9] L. Alexander, "Open-Source Information Reveals Pro-Kremlin Web Campaign," Global Voices, 13-Jul-2015. [Online]. Available: https://globalvoices.org/2015/07/13/open-source-information-reveals-pro-kremlin-web-campaign/. [Accessed: 08-Oct-2015].
[10] M. Bazzell, Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 4th ed. CCI Publishing, 2014.
[11] B. Etling, J. Kelly, R. Faris, and J. Palfrey, "Mapping the Arabic blogosphere: politics, culture, and dissent," Berkman Cent. Res. Publ., vol. 6, 2009.
[12] R. B. Standler, "Propaganda and How to Recognize it." RBS0, 02-Sep-2005.