Leveraging Social Network Analysis and Cyber Forensics Approaches to Study Cyber 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. Further, with the availability of inexpensive and ubiquitous mass communication tools like social media, disseminating false information and propaganda is both convenient and effective. Groups' use social media to coordinate cyber propaganda campaigns in order to achieve strategic and political goals, influence mass thinking, and steer behaviors or perspectives about an event. In this research, we study the Online Deviant Groups (ODGs) who created a lot of cyber propaganda that were projected against the NATO's Trident Juncture Exercise 2015 (TRJE 2015) on both Twitter and blogs. Anti-NATO narratives were observed on social media websites that got stronger as the TRJE 2015 event approached. Call for civil disobedience, planned protests, and direct action against TRJE 2015 propagated on social media websites. We employ computational social network analysis and cyber forensics informed methodologies to study information competitors who seek to take the initiative and the strategic message away from NATO in order to further their own agenda. Through social cyber forensics tools, e.g., Maltego, we extract metadata associated with propaganda-riddled websites. The extracted metadata helps in the collection of social network information (i.e., friends and followers) and communication network information (i.e., network depicting the flow of information such as tweets, retweets, mentions, and hyperlinks). Through computational social network analysis, we identify influential users and powerful groups (or, the focal structures) coordinating the cyber propaganda campaigns. The study examines 21 blogs having over 18,000 blog posts dating back to 1997 and over 9,000 Twitter users for the period between August 3, 2014, and September 12, 2015. These blogs were identified, crawled and stored in our database that is accessible through the Blogtrackers tool. Blogtrackers tool further helped us identify the activity patterns of blogs, keywords patterns, the influence a blog or a blogger has on the community, and analyze the sentiment diffusion in the community.

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

1 Introduction

Technology is evolving and this evolution changed the way we access information, express our opinion, or communicate with each other. The inexpensive nature, easy to use, and the popularity of social media made it a powerful tool that can be used to disseminate misinformation or coordinate cyber propaganda campaigns in order to achieve strategic and political goals, influence mass thinking, and steer behaviors or perspectives about an event. This motivated us to investigate these phenomenon's and conduct this research/study. For example, there were a lot of anti-NATO propaganda that were pushed by pro-Russian media that presented NATO's exercise (Trident Juncture Exercise 2015) as preparation for WW3, or acts of provocation for Russia, and these exercises were not defensive in nature but openly aggressive. Such propaganda was shared in many social media outlets such as blog sites[1], Twitter[2], or YouTube channels[3].

A study showed that cybercriminals tend to collaborate or even transact cyber-attack tools via the "dark markets" that exist in the online social media [1]. In addition to cyber criminals, deviant groups can also collaborate and conduct acts collectively using this market. We define Online Deviant Group (ODG) as a group of individuals that organizes a harmful activity using cyberspace in which its result would affect cyberspace, physical space or both i.e. the "Cybernetic Space" [2].

Social media such as blogs, Twitter, Facebook, Google Plus, Instagram, and the likes are rich sources of information [3]. With millions of social network users around the globe, cyber forensic analysis of social media has profound applications [4]. Cyber forensic analysis of social media sites can help collect evidence that helps investigators develop a strong case [3]. Cyber forensics 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" [5]. With the use of metadata, extracted using cyber forensics such deviant groups can be discovered. We develop methodologies that can be used to identify such deviant groups.

Digital forensics research can be categorized into two themes, *theoretical* and *technical*. Theoretical research covers the development of theories and methodologies including models, frameworks, and processes to conduct digital forensics investigations. A research was done by Lau et al. [1] in which they apply a probabilistic generative model to mine cyber criminal networks from online social media. Their model outperformed the Support Vector Machine (SVM) based method (by 16.62% Area Under the ROC Curve) and the Latent Dirichlet Allocation (LDA) based method (by 5.23% Area Under the ROC Curve) [1]. On the other hand, technical research covers

[1] Trident Juncture: NATO's Largest Military Exercise since Cold War. The "Fictitious Target" is Russia (GlobalResearch.ca, available at: `http://bit.ly/294Uo2E`)

[2] War game whoops! NATO exercises end with hovercraft, Humvees stuck in sand (VIDEO) (RT.com, available at: `http://bit.ly/298ya0R`)

[3] YOU WON'T BELIEVE WHAT NATO IS DOING TO PREPARE FOR WORLD WAR 3! (YouTube.com, available at: `http://bit.ly/29bcH7P`)

the development of tools and techniques to help in digital forensics investigations [6]. Collecting social media evidence is different than traditional digital forensics, which usually requires investigators to extract data from a piece of hardware in the possession. Social media providers like Facebook or Twitter are not going to help investigators get that evidence unless it is an extreme case [3] [4]. One of the problems in cyber forensics is how to visualize the collected cyber forensics data in an easy to understand format [4]. Some techniques an investigator might use is screencasts tools, such as Microsoft's Skydrive or Screencast-o-matic, which record whatever an investigator might see on social media [3].

In this work, we identify and study the behavior of coordinating deviant groups in social media during the cyber propaganda campaigns using social network analysis and cyber forensics techniques. For cyber forensics data, we use Maltego (available at: `https://www.paterva.com/web6/products/maltego.php`), which is a tool that can be used to gather any publicly available data that might provide an insight on how different social media platforms (e.g., blog sites connected to Twitter accounts) are connected or affiliated [7]. We use computational social network analysis in combination with the metadata extracted from the cyber forensics tool to have a comprehensive understanding of the entire propaganda campaign coordination.

For conducting social network analysis we use NodeXL [8] and focal structure analysis (available at: `http://www.merjek.com`). Focal structure analysis was implemented by Sen et al. [9] to 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. This approach was tested in many real world cases including the Saudi Arabian women's right to drive campaign (Oct26Driving campaign) on Twitter, and the 2014 Ukraine crisis when President Viktor Yanukovych rejected a deal for greater integration with the European Union [9]. For blog analysis, we use Blogtrackers (available at: `http://blogtrackers.host.ualr.edu/`) [10].

The implication of this research is not only interesting for the scientific community, but also for authorities as these deviant groups pose non-negligible concerns for public safety and national security, e.g., in many cases these groups call for civil disobedience, planned protests, or direct actions against specific events. Therefore, in this study, we propose to seek answers to the following questions that further help us analyze cyber propaganda campaigns:

1. Are there any blogs used by the groups to disseminate propaganda? How can we identify those blogs?
2. Who are the most coordinating/influential groups in the network? Which nodes are the most communicative, or most powerful to disseminate the message using their social ties? What are the most used platforms by the individuals in the group?
3. How is the propaganda resonating with the community? What is the public opinion mostly concerned about? What are the top tweets, top hashtags, etc.?

4. Who are the most important individuals in the network (active tweeters, most communicative nodes in the network)? Can we identify influential narratives in the cyber campaign?
5. Can we identify the coordinating Bots used during the propaganda campaign and study their content and behavior?

Seeking answers to the aforementioned questions, we make the following contributions in this article:

- We design social network analysis and social cyber forensics informed methodologies to study the sociotechnical behaviors of individuals during cyber propaganda campaigns to develop detection tools ready to be deployed for cyber operations.
- Provide a deeper understanding of social media as a facilitator for a group's activities to advocate a specific agenda.
- We were able to identify influential users on Twitter and blogs and find the relationship between them to study the cross-influence of various social media platforms in conducting strategic information maneuvers during cyber propaganda campaigns.

Rest of the chapter is organized as follows. Theoretical background of the research is discussed in Section 2. Section 3 presents the research methodology including two datasets used to study the cyber propaganda campaigns with different methodologies followed with each. Analysis done by our developed Blogtrackers tool is presented in Section 4 to examine the methodologies efficacy. Section 5 concludes the chapter with possible future research directions.

2 Literature Review

In this section, we review some of the literature that is relevant to this research and discusses how our work is different than the others. In section 2.1, we discuss some of the literature that has been done in the cyber forensics field particularly the evolution of the usage of digital forensics tools over time, then we discuss what the term "data carving" is, and finally, we discuss the forensics tools used to collect data from social networks. In section 2.2, we review some of the previous work done related to the usage of bots in information operations. In section 2.3, we review some of the work done on calculating the influence score in social media channels, e.g., Twitter and blogs.

2.1 Cyber Forensics

For the last three and half decades digital forensics tools have been evolved from simple tools, which were used mainly by law enforcement agencies to important tools for detecting and solving corporate fraud [11]. Cyber forensics tools are not a new type of tools but they are evolving over time to have more capabilities, more exposure

to the audience (investigators or public users), and the type and amount of data that can be obtained by using each tool. 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) and were written in `Assembly` language or `C` language with limited capabilities and less popularity. As time passed 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 become more popular and also have more capabilities, e.g., they can recover deleted files and fragments of deleted files such as *Expert Witness* and *Encase* [12]. Nowadays, many tools are available to the publics that enable them to collect cyber forensics data and visualize it in an easy to understand way, e.g., Maltego[4] tool.

Data carving is a term widely used in the field of cyber forensics which means "Identifying and recovering files based on analysis of file formats" [5]. Carving digital forensic data can play a vital role in solving digital crimes. A lot of research has been conducted to improve data carving [5]. According to Nadeem et al. [11] literature review on articles that are related to the digital investigation or computer forensics on *disk area*, more research is needed to improve data carving techniques to retrieve important data and evidence from damaged or corrupted data resources [11]. Although there is a big research thrust on *data carving* within the forensics area, however this is not exactly relevant to our research efforts, as we are not collecting forensics data from a disk or a device instead collecting metadata using forensics tools (i.e., Maltego) and techniques (e.g., websites unique identifiers, email addresses, or IP addresses among others).

Social network forensics tools collect data in many different ways, e.g., crawling by using the social network APIs, extract artifacts from local web browsers cache, sniffing on unencrypted Wi-Fi's (active attacks) or with ARP spoofing on LANs, or using a third party extension for the social network in combination with a traditional crawler component (friend in the middle attack) [4]. Another investigative tool that might be used is to hook into the APIs of social media such as Facebook or blogs and collect metadata of a blog entry or Facebook walls such as time stamps, affiliations, IP addresses, locations, or email addresses [3]. Research by Noora et al. [13] obtains cyber forensics evidence from social media applications that are installed on smartphones. Their research was testing whether the activities conducted through these applications were stored on the device's internal memory or not. They used three major social media apps, i.e., Facebook, Twitter, and MySpace and three devices types, i.e., iPhone, BlackBerry, and Android for their experiments. The results show that BlackBerry devices do not store any information that can be retrieved by digital forensics tools while iPhone and Android phones store a significant amount of valuable data that can be retrieved [13]. Some work focused on extracting forensics data of social media apps from the computer hard disk, e.g., carving artifacts left by the use of Facebook Chat on a computer's hard disk [14]. A novel method to harvest/collect/carve data from social network websites, e.g., Facebook, was introduced

[4] Maltego, available at: `www.paterva.com/web6/products/maltego.php`

by Markus et al. [15]. They designed a hybrid system that is based on a custom add-on for social networks in combination with a web crawling component. Their system is able to carve "*social snapshots*" which are defined as all the profile information of the target user, e.g., user data, messages, photos, and the associated metadata, e.g., internal timestamps and unique identifiers [15]. In our research, we are not creating a tool to collect forensics data from social networks instead we are using an open source tool called Maltego which is developed by Paterva[5]. Maltego is an open source tool that collects Open Source Intelligence (OSINT) and forensics data. This tool provides a library of transformations for the discovery of data from open sources. It helps analyze the real-world connections between groups, websites, and affiliations with online services such as Facebook, Flickr, and Twitter. It also provides the capability to extract and visualize the results in a graph format that is suitable for link analysis.

2.2 Empirical Observations and Trends of Bots Used in Information Operations

It has been widely observed that in a cyber propaganda campaign, alongside human actors, bots/botnets/Automated Social Actors (ASA) also participate in the dissemination of propaganda. It is, therefore, important to study the types, categories, and strategies that bots use to act as powerful propaganda dissemination tool during crises. An earlier study [16] reported that bots were used in a sophisticated manner to disseminate propaganda during the uprising of the Syrian civil war. The authors studied the "Syrian Social Bots" or (SSB) examining the content of the tweets and categorized the bots based on the content posted, the time before they get suspended, and type of activity the bot does (tweet or retweet). The study classified the bots into following types:

- **Core Bots which** have three categories:

  1. Short-Lived Bots: *retweet* a lot but seldom *tweet* and they lasted for *less than 6 weeks* before Twitter suspended the account,
  2. Long-Lived Bots: *retweet* a lot but seldom *tweet* and they lasted for *more than 25 weeks* before Twitter suspended the account, and
  3. Generator Bots: *tweet* a lot but seldom *retweet* anything.

- **Peripheral Bots:** accounts that participate in the dissemination process. Their task was *retweeting* one or more tweets *generated by the core bots*.

We did further investigation and studies to identify the types, strategies these bots uses, and categorize them. Toward this direction, we studied the bots used to disseminate ISIL's beheading video-related propaganda (i.e., the Egyptian Copts, the Arab-Israeli "Spy", and the Ethiopian Christians) [17] [18]. We also studied the bots used to disseminate propaganda during the Crimean water crises [19] and the Dragoon

[5] Paterva (Pty) Ltd a new train of thought, available at: `www.paterva.com`

Ride exercise [20]. We study two different bipartite networks, i.e., User-Texts and User-URLs, in addition to one-mode networks, i.e., communication network (tweets, retweets, and mentions network) and social network (friends/followers network). These studies resulted in the following findings:

- Botnets were used heavily in all the cases to disseminate propaganda.
- The tweets contain mainly hashtags or keywords that may or may not be related to the event and URLs that point to resources related to the propaganda (e.g., videos, images, and memes).
- Accounts were identified as ***bots*** if they have the following characteristics:
  - The content of the tweets contains a high frequency of URLs.
  - The names of the accounts are very similar.
  - Tweets a lot in short period of time.
  - The tweets contain characters usually a human user would not post.

We were also able to identify some of the information maneuver strategies that botnets use to disseminate their propaganda such as:

- 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 a crisis.
- Smoke Screening: when a bot would mention something about, for example, Russia or Ukraine, but not necessary related to the crises [19]. Similar techniques have been used in the Syrian Social Bot (SSB) to raise awareness of the Syrian civil war [16].
- Thread-Jacking: the change of topic in a "thread" of discussion in an open forum.
- Hashtag-Latching: strategically associating unrelated but popular or trending hashtags to target a broader, or in some cases a very specific audience.

2.3 Influence in Social Media

Blogs provide a rich medium for deviant groups to build and frame propaganda by using half-truth or twisting facts to influence the masses. On the other hand, Twitter is limited by its number of characters (i.e., 140 characters) is merely used as a dissemination medium or communication network. Instead, Twitter is used as a driving vehicle to steer the traffic of its audience, i.e., followers of the account to the blog sites where the blogger have no limitation on words for framing and disseminating propaganda over social media. It is important to understand the disinformation dissemination network on Twitter, but it is more important to understand the activity generated by the blog posts or the bloggers.

Identifying influential individuals is a well-studied problem. Many studies have been conducted to identify the influence of a blogger in a community [21] [22] [21] [23] [24] [25]. The basic idea of computing the influence a blogger has is to aggregate the influence of their individual blog posts. If a blog post has a lot of in-links and

comments then it indicates that the blogosphere has interest in this blog post. In-links and comments contribute positively towards the influence of the posts whereas out-links of the blog posts contribute negatively towards the influence. Hence, one way to compute influence is by a weighted linear equation of in-links, comments, and out-links of a blog post [22]. An alternate approach is to use a modification of Google page rank to identify influential posts as well as bloggers [24].

3 Methodology

In this empirical study of Anti-NATO and Anti-TRJE 2015 cyber propaganda campaign, we studied two types of datasets collected from two different sources, i.e., a dataset we collected using Twitter API through NodeXL and a dataset collected by Scraawl[6]. For each of these datasets, we followed a path of analysis based on the information available. The two paths of analysis are connected to have a comprehensive understanding of the cyber propaganda campaigns that were projected against TRJE 2015 exercise and NATO. **Fig. 1** depicts a flow chart of the methodology we followed in this study.

3.1 Dataset 1: Twitter Accounts of Historical Deviant Groups Known for Their Anti-NATO Narratives

A. Dataset Description

We identified six groups that 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 used 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 NodeXL to collect a network of *replies, tweets, mentions, 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 4:51:47 PM UTC to 9/12/2015 3:22:24 AM UTC. The dataset file we obtained contains: 10805 friends/followers, 68 replies, 654 tweets, 1365 mentions, 9129 total nodes, 10824 total edges (see **Fig. 2**).

B. Metadata Extraction Using Cyber Forensics Approaches

By using the Unique Identifier, e.g., Google analytics ID obtained by Maltego we can infer connections among blog sites. Maltego is an open source intelligence and forensics application. It saves a lot of time in mining and gathering of information as well as the representation of this information in an easy to understand format. *Google Analytics* is an online analytics tool 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

[6] Scraawl, available at: `www.scraawl.com`

account. The account has a unique identifying "UA" number, which is usually embedded in the website's HTML code [7]. Using this code other blog sites that are managed under the same UA number can be identified. This method was reported in

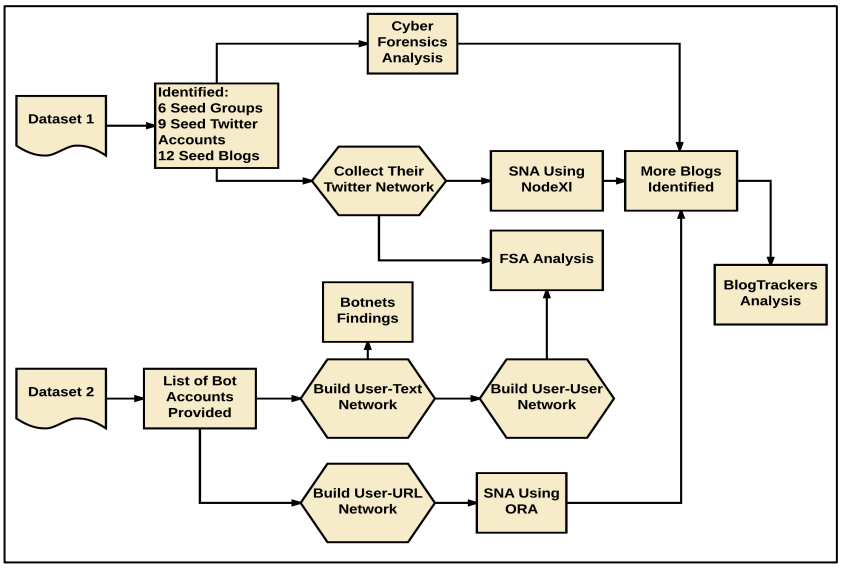

Fig. 1. Methodology to study the anti-NATO propaganda campaign

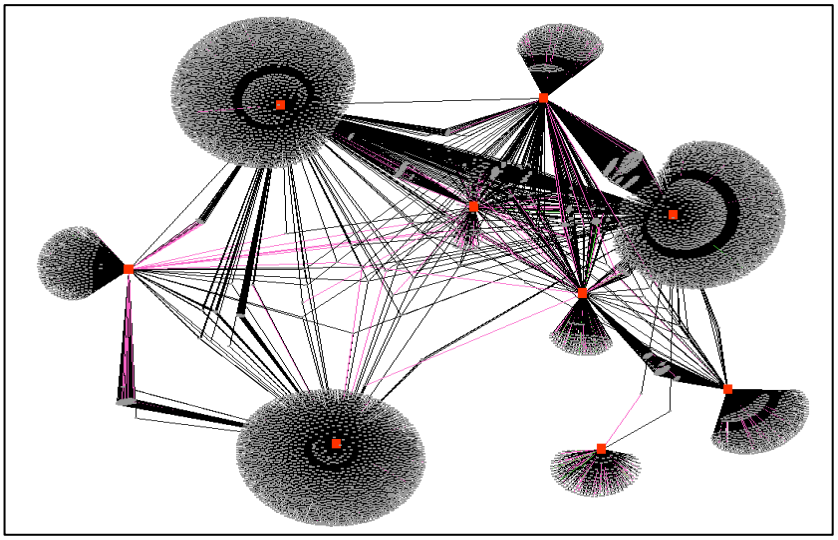

Fig. 2. Twitter social network of the 9 users identified from cyber forensic analysis. The 9 users identified are indicated in Red color and all other users are indicated in Gray color. *Friends and followers* edges are depicted in Black color, *mentions* relation depicted in Purple, *replies* depicted in Green, and *tweets* in Gray.

2011 by Wired, and also was cited in the book titled "Open Source Intelligence Techniques" by Michael Bazzell an FBI cyber crime expert [7] [26].

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 different 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* [27]. 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 (see **Fig. 3**). 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 the USA, and Cluster 3 has 12 blog sites located in Spain, Cayman Islands, UK, and Germany. The result is shown in **Fig. 3**. From initial 12 blog sites, we obtained 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.

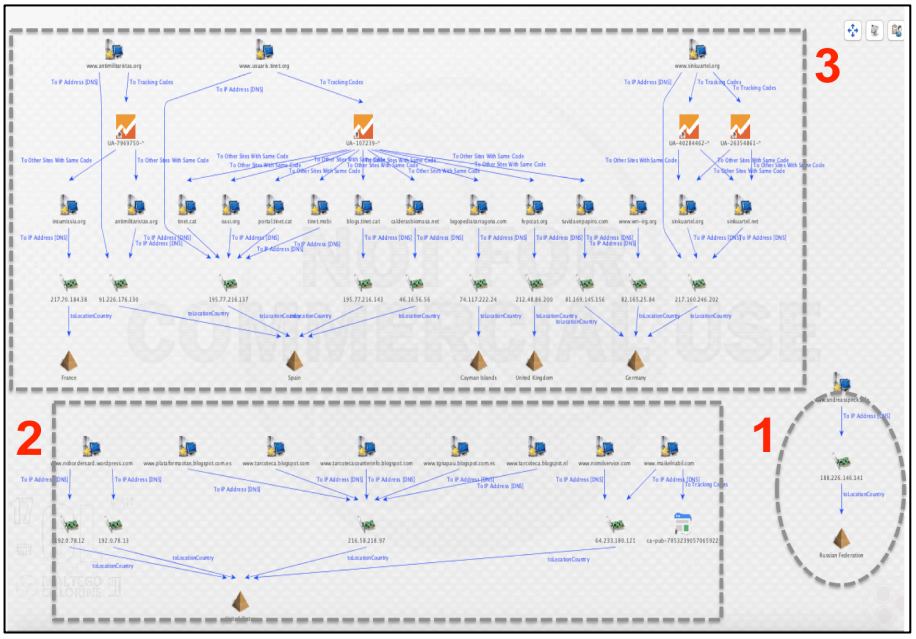

Fig. 3. Additional blog sites were identified using Maltego. Finding the IP addresses of all the blogs and their location gave us three clusters. Cluster 1 represents one blog site located in Russia, cluster 2 represents 8 blog sites located in the USA, and cluster 3 represents 16 blog sites located in Spain, Cayman Islands, UK, and Germany.

C. Applying Social Network Analysis to Identify Influential Information Actors

After finding other related blog sites used by the group to disseminate their propaganda using cyber forensics tool (Maltego) and methodology (unique identifier) we applied social network analysis to find who are the most important nodes in the entire graph by activity type. We also wanted to know the most used hashtags during the time of the exercise. This can help in targeting the audience who follow that hashtag if counter-narratives were necessary to be pushed to the same audience; the most tweeted URLs in the graph which gives an idea about the public opinion and concerns; and the domains used most in the entire graph that helps to know where the focus of analysis should be directed, or what other media platforms are used (see **Table 1**). Using NodeXL we were able to answer all the aforementioned questions, for example, two of the top 10 hashtags were used during the TRJE 2015 exercise were #YoConvoco (using Google translation service to English as "I invite") and #SinMordazas (using Google translation service to English as "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 shared the most in the data set collected reveals that these URLs were links to websites that are asking people for fiscal objection to military spending on wars from the income tax return. Exploring the top domains also help us identify more blogs to crawl that disseminate propaganda against TRJE 2015.

D. Applying Focal Structure Analysis (FSA) to Identify Powerful Groups of Individuals Effecting Cyber Propaganda Campaign

To study the cyber propaganda campaign further, we apply Focal Structures Analysis (FSA) approach to find the influential group of nodes. To find the most influential group of nodes in the network we divided our data file (9,129 nodes and 10,824 unique edges) into two types of networks namely, "Social network", derived from friends and follower's relations and "Communication network", derived from replies and mentions relations. We ran the FSA approach on these two networks to discover the most influential set of nodes or the seeders of information in the community.

Running FSA on the *social network* resulted in 1 focal structure with 7 nodes (see **Fig. 4**). 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 (see **Fig. 5**). 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.

Table 1. The most used URLs, Domains, and Hashtags used by the group to disseminate propaganda

Top URLs in Tweet in Entire Graph	Top Domains in Tweet in Entire Graph	Top Hashtags in Tweet in Entire Graph
http://bit.ly/1TSo024	fb.me	#cosymposium
http://bit.ly/1mpX3Z5	utopiacontagiosa.org	#yoconvoco
http://bit.ly/1Fhmxtw	bit.ly	#sinmordazas
http://bit.ly/1JeDzeL	wri-irg.org	#co
http://bit.ly/OFGM2015	com.es	#leyesmordaza
http://ow.ly/HcVkx	twitter.com	#siria
http://bit.ly/1dhJBkL	sinkuartel.org	#cos
http://j.mp/llamamiento	ow.ly	#coday
https://diasp.eu/posts/3493166	eldiario.es	#Egypt
http://bit.ly/1UFcIPD	diasp.eu	#Turkey

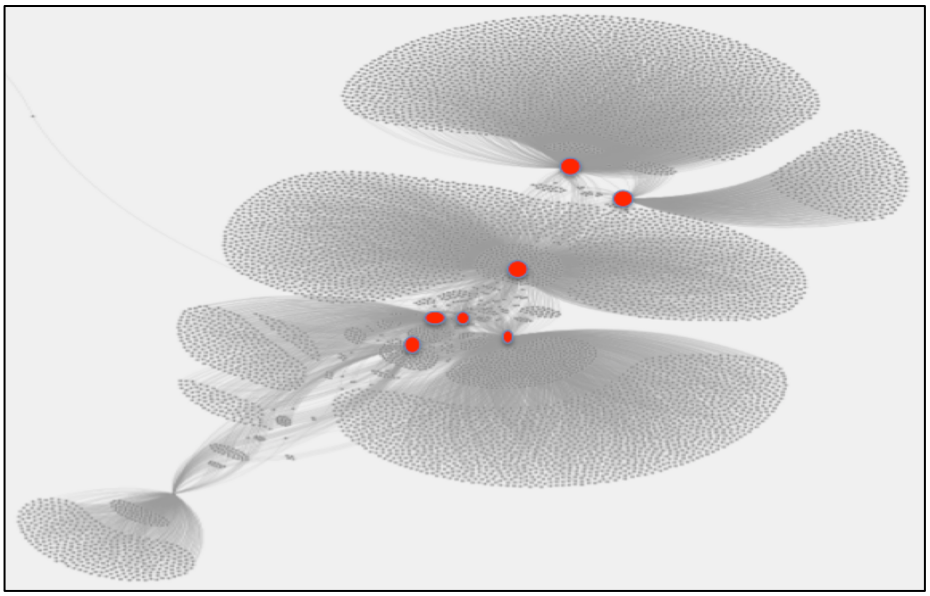

Fig. 4. Twitter social network of the 9 users with members of the single most important coordination structure indicated in Red color.

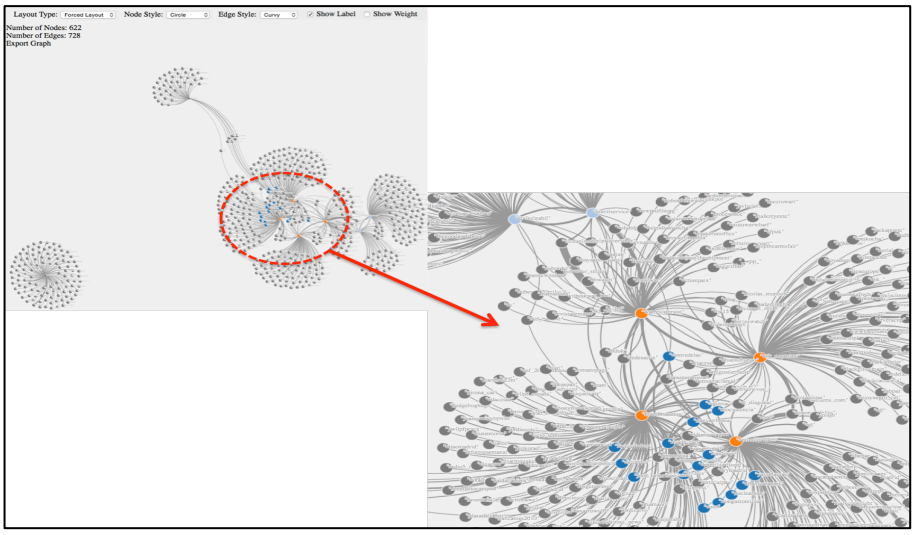

Fig. 5. Communication network (mentions, and replies network). Focal structure analysis approach helped in identifying a highly sophisticated coordinating structure, which is marked inside the red circle in the figure on top left. Upon zooming in on this structure (displayed on the bottom right), three focal structures were identified with 22 nodes. The color of the nodes represents the color of the focal structures.

E. Summary of the Conducted Analysis on Dataset 1:

- We collected the Twitter network an "Agent X Agent" network (both the "communication network" and the "social network") of the six seed deviant groups who had 9 twitter accounts. Then we analyzed this network to discover who are the agents/accounts/nodes that are top ranked in their activity, i.e., tweet, retweet, or mention the most. We also discovered the most used hashtags, the most tweeted URLs in the graph, and the domains that are used the most in the entire graph. This served as a *node level analysis*.
- Then we used cyber forensics tool and techniques to discover the hidden relationships between the other blog sites that are related to the seed blogs.
- Then we applied Focal Structure Analysis (FSA) to discover the coordinating groups. This served as *a group level analysis*.

3.2 Dataset 2: Twitter Accounts of the Anti-NATO Bots Used During the Cyber Propaganda Campaign

A. Dataset Description

This dataset was collected using the Scraawl tool. It was noticed that bots were used to speed up and amplify the propaganda campaigns. Scraawl tool identified around 218 bot accounts. Botnets' tweets, mentions, and retweets were collected. The data was collected for the period from October 8, 2015, to October 11, 2015, that resulted in 869,062 tweets, 37,042 mentions, 74,898 retweets, and 308 unique users.

B. Applying Social Network Analysis to Identify Influential Bots

We constructed two types of networks viz. User-URLs (two-mode network, i.e., "Agent by Knowledge" network where agent is the Twitter account and the knowledge, in this case, is the URLs contained in the tweets) and User-Texts (two-mode network, i.e., "Agent by Knowledge" network where agent is the Twitter account and the knowledge in this case is the whole text collected including the tweets, retweets, and mentions). For the ***User-URLs*** network, we used ORA NetScenes[7] to extract the top 20 tweeted URLs, mentioned URLs, and retweeted URLs. This network enabled us to find out that:

- Many of the URLs in the top 20 **Mentioned** URLs, were mainly talking about NATO and the TRJE 2015 (propaganda dissemination). So more attention should be given to the *mentions network*.
- We identified two of the top 20 **Tweeted** URLs as interesting URLs because these websites show Ukraine and Russian Trending Topics/Hashtags on Twitter. This is an indication of tools that these bots use to get the most trending hashtags associated with the content of their tweet so they can reach wider audience (Hashtag-Latching).
- Most of the top 20 **Tweeted** URLs were NOT of relevance to NATO or the TRJE 2015. Most of the URLs were spam, e.g., gambling websites, coupons websites, food recipes, Android TV app, or a Turkish website helps users gain followers.
- The top 20 **Retweeted** URLs were NOT of relevance to NATO or the TRJE 2015. Most of these URLs were from Greek or Italian news websites talking about the Turkish Election.

We used the blogs identified above as our initial seed of blogs to discover other blogs that are related/affiliated with them using Maltego. Then all these blogs are crawled and fed to Blogtrackers tool to perform more analysis. We also constructed a ***User-Texts*** network and we discovered the following:

- Many users are **tweeting** the same tweet content. This is considered as unusual behavior as it is almost impossible for two people to write the same exact text without a single punctuation difference unless they have a prior communication or same source of message. This behavior is an indication of "Clone Accounts" or "Echo Chamber".
- We also have noticed that some of the bots that participated in TRJE2015 propaganda dissemination also participated in the past in other crises such as the Crimean Water Cries and the propaganda disseminated during the Dragoon Ride Exercise [20].
- Most of the strategies mentioned in section 2.2 were used in disseminating the propaganda, e.g., Hashtag-Latching.
- Some users were repeatedly top-ranked in the node-level measures calculated by ORA, which are:

[7]ORA NetScenes, available at: `http://bit.ly/27fuHnv`

- **Capability**: Detects entities with high or low degree relative to other entities.
- **Centrality-Out-Degree**: For any node, e.g., an individual, the out links are the connections that the node of interest has to other nodes. For example, imagine an agent by knowledge network where the number of out-links an agent would have is the number of pieces of knowledge it is connected to. The scientific name of this measure is out-degree and it can be calculated on any network. Individuals or organizations that are high in out-degree for knowledge have more expertise or are associated with more types of knowledge than are others.
- **Centrality-Row Degree**: Number of ties to others. Row sums of adjacency matrix.
- **Cognitive Distinctiveness**: Measures the degree to which each pair of agents has complementary knowledge, expressed as the percent of total knowledge.
- **Cognitive Expertise**: Measures the degree to which each pair of agents has complementary knowledge, expressed as a fraction of the knowledge of the first agent.
- **Cognitive Resemblance**: Measures the degree to which each pair of agents has the exact same knowledge. The number of knowledge bit normalizes each value.
- **Cognitive Similarity**: Measures the degree to which each pair of agents has overlapping knowledge.
- **Correlation-Distinctiveness**: Measures the degree to which each pair of rows has complementary data, expressed as *the percent of total data*.
- **Correlation-Expertise**: Measures the degree to which each pair of rows has complementary data, expressed as *a fraction of the data of the first row*.
- **Correlation-Resemblance**: Measures the degree to which each pair of rows has the exact same bits. The number of columns normalizes each value.
- **Correlation-Similarity**: Measures the degree to which each pair of rows has overlapping data.
- **Exclusivity**: Detects entities that have ties that comparatively few other entities have. Individuals or organizations that are high in exclusivity for knowledge are those that have expertise or are connected to types of knowledge that few others have.
- **Exclusivity-Complete**: Detects entities that have ties that no other entities have. Individuals or organizations that are high in complete exclusivity for knowledge are those that have expertise or are connected to types of knowledge that no one else has.
- **Exclusivity-Knowledge**: Detects agents who have knowledge that few other agents have.

This is an indication of how powerful these nodes are in the network. For example, we were able to identify many accounts that participated in other propaganda campaigns during other exercises, e.g., the Dragoon Ride Exercise. The ranks of these nodes are shown in **Fig. 6**.

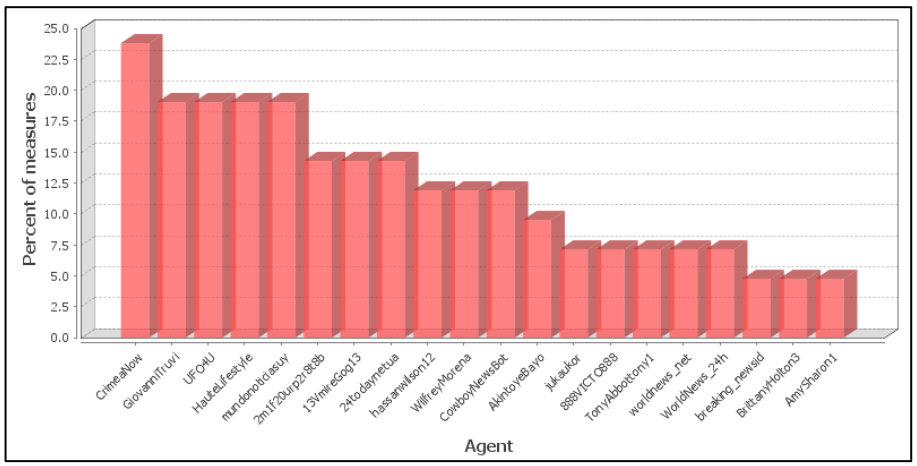

Fig. 6. The recurring top-ranked Agents chart shows the Agent that is repeatedly top-ranked in the node-level measures mentioned above. The value shown is the percentage of measures for which the Agent node was ranked in the top three.

C. Applying Focal Structure Analysis to Identify Powerful Bots Effecting Cyber Propaganda Campaign

We extracted the users mentioned and retweeted from the text to construct a one-mode (Agent by Agent) communication network (edges represent retweets, and mentions, note that the tweets were not included in this network because in this case they are self-loop edges and do not add any meaning in this case). This resulted in a network contains 18, 987 nodes and 23, 824 edges. Then we applied FSA algorithm to find the coordinating bots. This resulted in 15 focal structures (a strongly influential group of nodes) that include 286 nodes in total (see **Fig. 7**). Five accounts from the top 20 ranked nodes were also in the identified FSAs. This means that these accounts are not just top-ranked in the Agent by Knowledge network but also coordinating accounts in the communication network (this gives them more importance).

D. Summary of the Conducted Analysis for Dataset 2:

- We created an "Agent by Knowledge" network to see who are the nodes/agents who are top ranked in the *node level measures* aforementioned in section B. This gives us an insight on the important nodes in the network (or the active nodes during the propaganda dissemination). In other words, the nodes that share more knowledge (in this case tweet more), or nodes that mention more users in their tweets have a higher participation rate in the dis-

cussion than other nodes. Also, the nodes that retweet a lot more than other nodes are those who are interested in spreading the messages to a wider audience. This serves as *node level analysis*.

- We also created an "Agent by Agent" *communication network* then we applied the Focal Structure Analysis to discover the coordinating groups. It is important to know the important/influential/coordinating groups in the network. These nodes have so much power by acting together they will be able to spread the message and be effective during propaganda campaigns. This is *a group level analysis*.
- As expected some of the nodes that are top ranked in the "Agent by knowledge" network were also in the focal structures. This gives these nodes more importance.

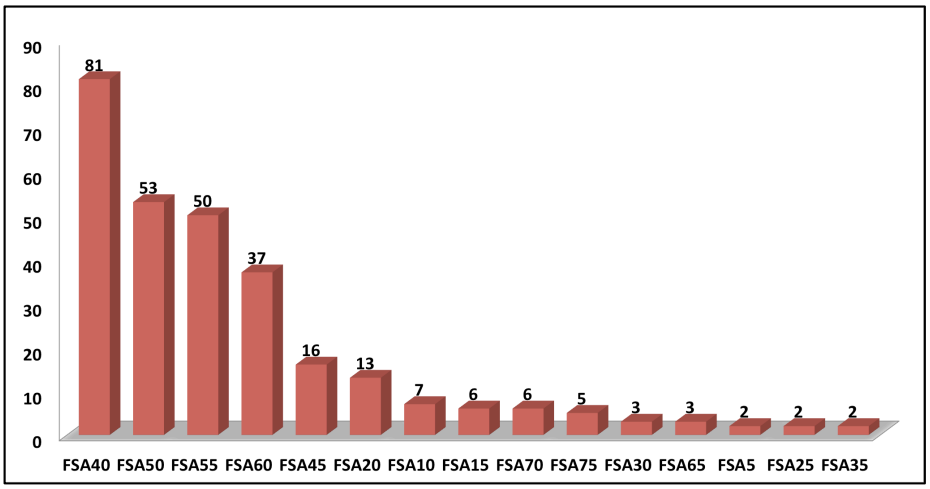

Fig. 7. The distribution of nodes among different focal structures. Here the FSA with ID = 40 has the highest number of nodes in it. The ID is used to distinguish each FSA and it is increasing in amount of 5.

3.3 Blogs Data Analysis and Findings

A. Dataset Description

Using the SNA and cyber forensic techniques mentioned in the previous sections we were able to identify more than 21 blogs site that disseminated propaganda against NATO and their TRJE 2015 exercise. We trained web crawlers using Web Content Extractor (available at: `http://bit.ly/1uUtpeS`) to collect data from these blogs. Upon crawling them we obtained a total of 15, 278 blog posts. These blogs were mainly located in the USA (we also have blogs located in Spain, Canada, Russia, Germany, UK, and Palestine). The location of the blog site was determined either from the IP address location obtained from Maltego or if the author explicitly mentioned in his blogs where s/he is living. The majority of the blog posts were written in

English language while posts in other languages were also collected, i.e., Spanish, Italian, German, Catalan, Arabic, French, Basque, Portuguese, and Russian.

B. Using Blogtrackers for Analysis

We started exploring the collected dataset by generating the *posting frequency* graph (depicted in **Fig. 8**) using Blogtrackers (available at: `http://blogtrackers.host.ualr.edu/`), for the period of August 2014 to December 2015. We observed a comparatively higher activity in these blogs from September 2015 to December 2015, the period around the Trident Juncture Exercise (TRJE 2015).

We generated *a keyword trends* graph for the keywords 'anti nato', 'trident juncture', 'nato' using Blogtrackers (depicted in **Fig. 9**). The keyword trend for the 'anti nato' completely aligned with the posting frequency graph in **Fig. 8** 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. We also found out that several blogs called for 'anti-NATO' protests and movements.

We developed a *sentiment trend* (depicted in **Fig. 10**) for the same period that confirmed our findings, i.e., more negative sentiment was observed than positive sentiment. Also, the number of blogs with negative sentiment was significantly more than blogs with positive sentiment.

We also ran the *Influential Posts* analysis [21] [22] in Blogtrackers to identify posts with high influence. Influence score of a post is computed using a stochastic model involving four factors, viz., *inbound links*, *outbound links*, *comments*, and *eloquence* of the blog post [21] [22] [23] [24] [25].

We found out that the *most influential posts* were from a blog site that was written in Italian language. Upon translation we found the post to be highly propaganda-riddled posts. It was demanding people to protest against the exercise conducted by NATO. The Blogger of this blog used two of the conventional propaganda techniques called "**Name Calling**" [28] (associating a negative word to damage the reputation) and "**Plain Folks**" [28] (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 it was exploiting resources. It also categorizes this exercise as an act of militarization of territories to train for war.

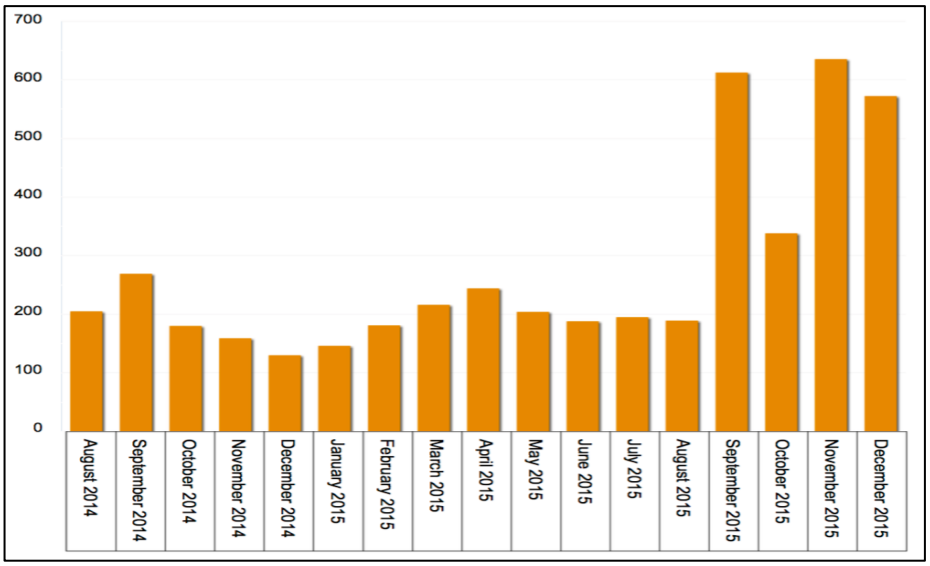

Fig. 8. The posting frequency graph generated by Blogtrackers shows an increase in the activity of blogs before TRJE 2015.

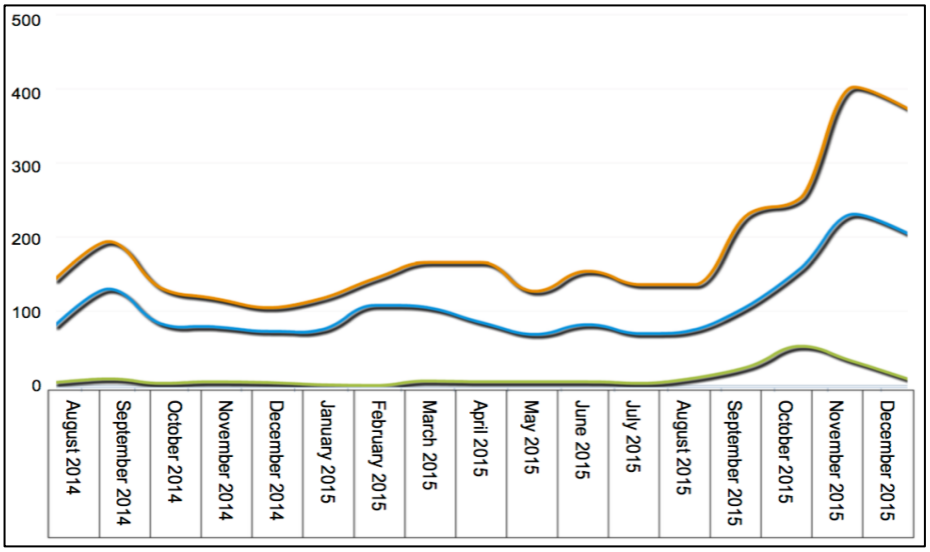

Fig. 9. Keyword trends for ‘anti nato’, ‘nato’, ‘trident juncture’ generated by Blogtrackers depicting the occurrence of these keywords over the time period.

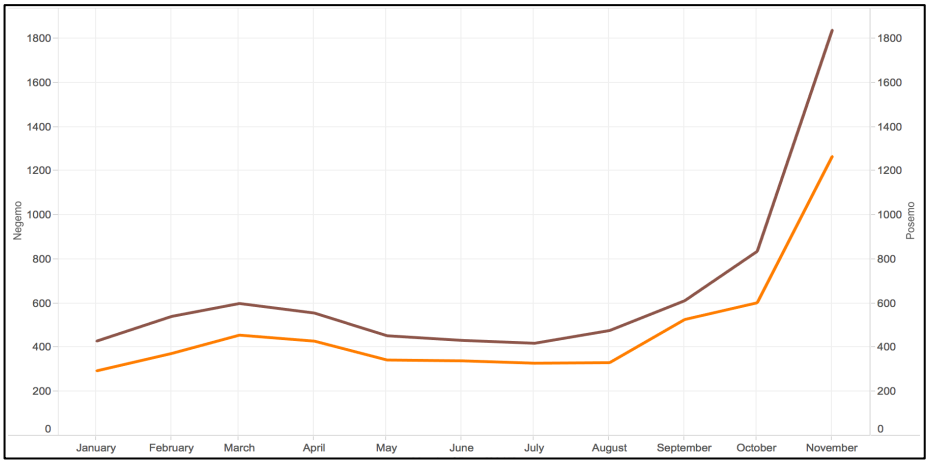

Fig. 10. Sentiment trends in the collected blogs.

4 Conclusion and Future Directions

In conclusion, the affordability and easy to use nature of social media gave it popularity to many people around the globe. The usage of social media meant to be for entertainment and to act as a mean of social communication environment but deviant groups harnessed this usage. Instead, they used it as a powerful tool to disseminate misinformation or coordinate cyber propaganda campaigns in order to achieve strategic and political goals, influence mass thinking, and steer behaviors or perspectives about some events. The latest behavior motivated us to do more investigation, study this phenomenon, and the behavior of the groups who conduct such acts.

In this work, we identify and study the behavior of coordinating deviant groups who created a lot of cyber propaganda against the TRJE 2015 on both Twitter and blogs. We utilized social network analysis, cyber forensics tools, and cyber forensics techniques to uncover the relation between the groups and to discover more groups. We design these informed methodologies to help develop detection tools ready to be deployed for cyber operations. We were able to identify influential users on Twitter (who use twitter as a tool to steer their followers on Twitter to their blog sites) and blogs and discover how they are connected/related to study the cross-influence of various social media platforms in conducting strategic information maneuvers during cyber propaganda campaigns. The aforementioned methodologies constitute a tiny but promising sample of an entire spectrum of approaches to extract metadata and relevant blog sites via cyber forensics. This set of methodologies would help in focused data collection, or guided snowball data collection, which then leads to the next phase of the study, i.e., a streamlined identification of key actors or bloggers that are top opinion leaders and top opinion disseminators.

For future work, we plan to focus on the messages that such groups are trying to spread. More precisely, we plan to do topic modeling of the messages to extract topi-

cal sentiments and targeted sentiments, to further enhance propaganda extraction. In addition to that, since some of the nodes that are top ranked in the "Agent by knowledge" network were also in the focal structures, which gives these nodes more importance, we are planning to find out the nature of such nodes (i.e., are they bots or regular users?) and what makes them so special that they appear in both networks, e.g., what type of tweets they do (e.g., tweet news URLs, or use more hashtags than regular users, etc.), what type of activity (tweet, retweet, mention, or reply) they do most, the frequency of tweets posted, etc. Also, since blogs do not have any constraints on the number of characters unlike Twitter, they afford a platform conducive for framing narratives. We, therefore, plan to analyze blog-originated propaganda techniques from a communication and information science perspective for the modern social information and communication systems. Further, we plan to improve Blogtrackers' capability to scale with copious amounts of blog data and have more functionality.

Acknowledgements: This research is funded in part by the U.S. National Science Foundation (IS-1636933, IIS-1110868 and ACI-1429160), U.S. Office of Naval Research (N000141010091, N000141410489, N0001415P1187, N000141612016, and N000141612412), U.S. Air Force Research Lab, U.S. Army Research Office (W911NF-16-1-0189), U.S. Defense Advanced Research Projects Agency (W31P4Q-17-C-0059) and the Jerry L. Maulden/Entergy Fund 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 organizations. The researchers gratefully acknowledge the support.

References

[1] R. Y. K. Lau, Y. Xia, and Y. Ye, "A Probabilistic Generative Model for Mining Cybercriminal Networks from Online Social Media," *IEEE Comput. Intell. Mag.*, vol. 9, no. 1, pp. 31–43, Feb. 2014.

[2] S. Al-khateeb and N. Agarwal, "Analyzing Flash Mobs in Cybernetic Space and the Imminent Security Threats A Collective Action Based Theoretical Perspective on Emerging Sociotechnical Behaviors," in *2015 AAAI Spring Symposium Series*, 2015.

[3] B. Wright, "Social Media and the Changing Role of Investigators," *Forensic Mag.*, Dec. 2012.

[4] M. Mulazzani, M. Huber, and E. Weippl, "Social network forensics: tapping the data pool of social networks," presented at the Eighth Annual IFIP WG, 2012, vol. 11.

[5] D. Povar and V. K. Bhadran, "Forensic Data Carving," in *Digital Forensics and Cyber Crime*, vol. 53, Springer Berlin Heidelberg, 2011, pp. 137–148.

[6] S. Saleem, P. Popov, and I. Bagilli, "Extended abstract digital forensics model with preservation and protection as umbrella principles," presented at the 18th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems - KES2014, Gdynia, Poland, 2014, vol. 35, pp. 812–821.

[7] L. Alexander, “Open-Source Information Reveals Pro-Kremlin Web Campaign.” Global Voices, 13-Jul-2015.

[8] M. A. Smith *et al.*, “Analyzing (social media) networks with NodeXL,” in *Proceedings of the fourth international conference on Communities and technologies*, 2009, pp. 255–264.

[9] 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.

[10] N. Agarwal, S. Kumar, H. Liu, and M. Woodward, “BlogTrackers: A Tool for Sociologists to Track and Analyze Blogosphere.,” presented at the ICWSM, 2009.

[11] 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.

[12] K. Oyeusi, “Computer Forensics,” London Metropolitan University, 2009.

[13] N. Al Mutawa, I. Baggili, and A. Marrington, “Forensic analysis of social networking applications on mobile devices,” vol. 9, ELSEVIER, 2012, pp. S24–S33.

[14] N. Al Mutawa, I. Al Awadhi, I. Baggili, and A. Marrington, “Forensic artifacts of Facebook’s instant messaging service,” presented at the 2011 International Conference for Internet Technology and Secured Transactions (ICITST), 2011, pp. 771–776.

[15] M. Huber, M. Mulazzani, M. Leithner, S. Schrittwieser, G. Wondracek, and E. Weippl, “Social Snapshots: Digital Forensics for Online Social Networks,” presented at the Proceedings of the 27th annual computer security applications conference, ACM, 2011, pp. 113–122.

[16] N. Abokhodair, D. Yoo, and D. W. McDonald, “Dissecting a Social Botnet: Growth, Content and Influence in Twitter,” in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 2015, pp. 839–851.

[17] S. Al-khateeb and N. Agarwal, “Examining Botnet Behaviors for Propaganda Dissemination: A Case Study of ISIL’s Beheading Videos-Based Propaganda,” presented at the Data Mining Workshop (ICDMW), 2015 IEEE International Conference on, 2015, pp. 51–57.

[18] S. Al-khateeb, M. Hussain, and N. Agarwal, “Exploring ISIL Cyber Network Activities: Evolution, Means, and Strategies,” in *XXXVI International Sunbelt Social Network Conference*, Newport Beach, CA, p. 4.

[19] S. Al-khateeb and N. Agarwal, “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,” *J. Balt. Secur.*, vol. 2, no. 1, pp. 6–17, 2016.

[20] N. Agarwal, S. Al-khateeb, R. Galeano, and R. Goolsby, “Examining the Use of Botnets and their Evolution in Propaganda Dissemination,” *Def. Strateg. Commun.*, vol. 2, no. 2, pp. 87–112, Spring 2017.

[21] N. Agarwal, H. Liu, L. Tang, and S. Y. Philip, “Modeling blogger influence in a community,” *Soc. Netw. Anal. Min.*, vol. 2, no. 2, pp. 139–162, 2012.

[22] 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.

[23] S. Kumar, R. Zafarani, M. A. Abbasi, G. Barbier, and H. Liu, “Convergence of influential bloggers for topic discovery in the blogosphere,” in *Advances in Social Computing*, Springer, 2010, pp. 406–412.

[24] A. Java, P. Kolari, T. Finin, and T. Oates, “Modeling the spread of influence on the blogosphere,” in *Proceedings of the 15th international world wide web conference*, 2006, pp. 22–26.

[25] K. E. Gill, “How can we measure the influence of the blogosphere,” in *WWW 2004 Workshop on the Weblogging Ecosystem: Aggregation, Analysis and Dynamics*, 2004.

[26] M. Bazzell, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*, 4th ed. CCI Publishing, 2014.

[27] B. Etling, J. Kelly, R. Faris, and J. Palfrey, “Mapping the Arabic blogosphere: politics, culture, and dissent,” *Berkman Cent. Res. Publ.*, vol. 6, 2009.

[28] R. B. Standler, “Propaganda and How to Recognize it.” RBS0, 02-Sep-2005.