Studying the Weaponization of Social Media: Case Studies of Anti-NATO Disinformation Campaigns

Katrin Galeano, Rick Galeano, Samer Al-Khateeb, and Nitin Agarwal

Abstract Social media provides a fertile ground for any user to find or share information about various events with others. At the same time, social media is not always used for benign purposes. With the availability of inexpensive and ubiquitous mass communication tools, disseminating false information and propaganda is both convenient and effective. In this research, we studied Online Deviant Groups (ODGs) that conduct cyber propaganda campaigns in order to achieve strategic and political goals, influence mass thinking, and steer behaviors or perspectives about an event. We provide case studies in which various disinformation and propaganda swamped social media during two NATO exercises in 2015. We demonstrate ODGs' capability to spread anti-NATO propaganda using a highly sophisticated and well-coordinated social media campaign. In particular, blogs were used as virtual spaces where narratives are framed. And, to generate discourse, web traffic was driven to these virtual spaces via other social media platforms such as Twitter, Facebook, and VKontakte. By further examining the information flows within the social media networks, we identify sources of mis/disinformation and their reach, i.e., how far and how quickly the mis/disinformation could travel and consequently detect manipulation. The chapter presents an in-depth examination of the information networks using social network analysis (SNA) and social cyber forensics (SCF) based methodologies to identify prominent information brokers, leading coordinators, and information competitors who seek to further their own agenda. Through SCF tools, e.g., Maltego, we extract metadata associated with disinformation-riddled websites. The extracted metadata helps in uncovering the implicit relations among various ODGs. We further collected the social network of various ODGs (i.e., their friends and followers) and their communication network (i.e., network depicting the flow of information such as tweets, retweets, mentions,

K. Galeano · R. Galeano · N. Agarwal (✉)
Department of Information Science, University of Arkansas at Little Rock, Little Rock, AR, USA
e-mail: kkaniagalea@ualr.edu; ragaleano@ualr.edu; nxagarwal@ualr.edu

S. Al-Khateeb
Department of Journalism, Media, and Computing, Creighton University, Omaha, NE, USA
e-mail: sameral-khateeb1@creighton.edu

M. A. Tayebi et al. (eds.), *Open Source Intelligence and Cyber Crime*, Lecture Notes in Social Networks, https://doi.org/10.1007/978-3-030-41251-7_2

and hyperlinks). SNA helped us identify influential users and powerful groups responsible for coordinating the various disinformation campaigns. One of the key research findings is the vitality of the link between blogs and other social media platforms to examine disinformation campaigns.

Keywords Social media · Weaponization · Cyber forensics · Social network analysis · NATO · Disinformation

1 Introduction

Global communication has accelerated through the use of social media platforms over the past decade and in turn, this social media craze has affected demographics across the globe. An observation made in 2016 while living in The Netherlands, was that of school-age children pedaling their bicycles through busy city streets and staring at the screens of their phones. It even appeared that they were responding to messages while riding their bikes. Just a few years ago, this would have been unheard of, but it is ever present just driving down the street in any city now to see people driving vehicles and texting, posting updates, or even surfing the web.

The youth of yesteryear are the savvy technology operators of today. The kids that grew up playing the Atari 2600 or the Commodore 64 systems have revolutionized the way people communicate in our general day to day lifestyles; can you imagine how our communications cycle will look twenty-five years from now with the millennials that text and ride their bikes at the same time! For example, prior to the home video game industry, electronic gaming was more of a social setting that happened via coin-operated machines at an arcade or the pinball machine at the bar. "Atari bridged the gap, they moved video games from these places to the home. In so doing, they caused a market shift. [They realized] if you're only selling games per play to people in bars, then you're missing out on a whole marketplace of families and kids," Bogost said [1].

Transferring from the mindset of the 'home-based' video gaming world into the modern age of social media communications, look at the CEO of Facebook, Mark Zuckerberg. Facebook had its roots with Atari systems. At the age of twelve, Mr. Zuckerberg created "Zucknet" that was used in his father's dental office. Zucknet was a social messaging network designed to share data on patients and inform hygienists that patients were in the waiting room; essentially "Zucknet" was the grandfather of Facebook [2]. Mindful that not all social media platforms have a kinship to the home video game industry, they do have the universal notion of providing social conversations, sharing, and a gathering point for online business and personal communications. All too often, social media is used as the medium for the change agent. In this case, it does not necessarily represent an individual person but rather a larger concept. The change agent seeks to control the narrative.

Controlling the narrative; irrelevant to the platform, dates back to the 3rd century B.C. at the Platonic Academy in Greece. Aristotle's approach with his three appeals

about the general means of persuasion: (1) Logos (logic/reason/proof) (2) Ethos (credibility/trust), and (3) Pathos (emotions/values) have morphed into modern day disinformation campaigns via digital platforms. Controlling the narrative via mass influx of messaging into the information environment or simply being the first to input information—EVEN IF IT IS FALSE—has been able to gain momentum expeditiously.

This has developed into controlling the narrative via social communications. Social communication happens online, at a business meeting and even in classrooms. Influencing an audience through narrative is effective; for example, Amazon's founder and CEO has required executive meetings be switched to a storytelling approach via the "narrative structure" [3]. Jeff Bezos has banned PowerPoints during executive meetings, rather, "... he revealed that the "narrative structure" is more effective than PowerPoint" [3]. These examples of storytelling are even more attentive on social media and are oftentimes told by networks of [initially] organized trolls[1]. The rhetoric of communications through storytelling often mimics manipulative behaviors in order to influence the opinion of the audience by seeking to create an interest with the audience that keeps their attention. Otherwise, what good is storytelling with no one to tell the story to?

Studies have shown that public opinion is going to be more effective than bullets and bombs in the future war. Public opinion has become a tool to achieve a goal, may it be favoritism or turmoil. Information warfare can be used to change and shape public opinion, as it was the case during the Ukraine conflict during which the Russian public was influenced in believing that Russia was defending itself while the West was to blame for the conflict [4]. Influence campaigns can also easily be used to create friction aimed at weakening an adversary as demonstrated by the foreign interference of the U.S. 2016 presidential election [5]. Countering ODG mentality is a must to win the new battle of ideas. Today, transnational terrorist groups know that opinions can be influenced and they are using sophisticated techniques to overcome the time and space limitations of conventional influence campaigns by using digital tactics that take advantage of the speed and reach of the Internet. A study conducted by the Defense Academy of the United Kingdom [6] examines the sharing of the beheading videos of hostages by Al-Qaeda as an instance of strategic communication, defined as: "A systematic series of sustained and coherent activities, conducted across strategic, operational and tactical levels, that enables understanding of target audiences, identifies effective conduits, and develops and promotes ideas and opinions through those conduits to promote and sustain particular types of behaviour" [6].

Taking advantage of storytelling via blogs or social networking sites has quickly moved into strategic narratives and the framework for communications. Studying social media networks to identify false narratives or fake news has become easier because of the new digital information environment. Access to data reveals networks

[1] A person who disseminates provocative posts on social media for the troll's amusement or because (s)he was paid to do so.

operating in their true nature, often the networks are extremely large, numbering hundreds of thousands of nodes and ties. Steve Borgatti, a renowned social scientist implies that the importance of an organization in a given network is determined by the institutional affiliations it has within the network [7]. The flow of information amongst the institutional affiliates illuminate areas that are not identified without the use of exploratory social network analysis. *Illuminating these affiliations within networks was conducted through the combination of social network analysis and social cyber forensics. These two approaches allowed us to dissect the network, review the narrative approaches, and study how the authors created disagreement amongst the audience and swayed opinions.*

In this chapter, two different networks of online deviant groups (ODGs) are provided as case studies. The first is the North Atlantic Treaty Organization (NATO) Trident Juncture 2015 exercise and the second is the U.S. Army Europe Operation Dragoon Ride 2015. The focus of this chapter is to identify key actors and clusters within the overall networks and to be able to identify and illuminate these dark networks using social network analysis (SNA) and social cyber forensics (SCF). Malcolm Sparrow, emphasized that intelligence agencies do not have the expertise to conduct SNA, "social network analysis has a lot to offer intelligence agencies in this area through its ability to discover who is *central* within organizations, which individual's removal would most effectively disrupt the network, what role individuals are playing, and which relationships are vital to monitor" [8]. In general, this study provides an academic research background to further develop SNA and SCF based methods and procedures for those seeking the truth. Remember, "The main work of a trial attorney is to make a jury like his client." [9]. Our research demonstrates in both studies that the main actor was the trial attorney and the audience was the jury, easily persuaded to follow, like, retweet, and support the social narrative.

2 Literature Review

For this chapter we have reviewed literature of the work that has been previously conducted in the areas of *bots, cyber forensics*, and *SNA*. Specifically, we explain the background of bot research, data carving, and how cyber forensics is used with SNA. Lastly, a review is conducted on the influence assessment in the blogosphere. One of the aforementioned references in the introduction refers to how modern approaches to developing the narrative are being explored. Corporations that fuse social science into the business place are likely to have a competitive edge in their respective markets. A simple search of Amazon's available job postings as of May 13, 2018, showed multiple social science positions. Some of the preferred qualifications for a position as the Senior Research Psychologist identified "...research background in social or cognitive psychology or affective science, particularly with ties to motivation: deep knowledge of regressions, analysis of variance, multilevel models, structural equation models" [10]. Just this example alone provides a basis for

continued research in this field as the job market dictates more and more positions to shape behavior change in the future. Reviewing even literature online in a non-traditional sense such as "job postings" allows us an alternative approach to identify the relevance of this field.

Bots Automated social actors/agents or bots are not a new phenomenon. They have been studied previously in literature in a variety of domains, such as Internet Relay Chat (IRC) [11], online gaming, e.g., World of Warcraft (WoW) [12], and more recently behavioral steering through misinformation dissemination on social media [13]. One of the earliest bots emerged in 1993 in an internet protocol that allows people to communicate with each other by text in real time called Eggdrop. This bot had very simple tasks to welcome new participants and warn them about the actions of other users [11]. Shortly thereafter, the use of bots in IRC became very popular due to the simplicity of the implementation in and their ability to scale IRCs [14]. Both evolved over time and the tasks these bots were assigned became more complicated and sophisticated.

Abokhodair et al. studied the use of social bots regarding the conflict in Syria in 2012 [15]. The study focused on one botnet (i.e., a set of bots working together) that lived for six months before Twitter detected and suspended it [15]. The study analyzed the life and the activities of the botnet. Focus was placed on the content of tweets, i.e., they classified the content of the tweets into 12 categories: news, opinion, spam/phishing, testimonial, conversation, breaking news, mobilization of resistance/support, mobilization for assistance, solicitation of information, information provisioning, pop culture, and other. Through their research, the authors were able to answer the question on how the content of the bot tweeting in Arabic or English differ from the non-bot or legitimate users tweeting in Arabic or English? For example, bots tend to share more news articles, less opinion tweets, no testimonial tweets, and less conversational tweets than any other legitimate Arabic or English Twitter user [16]. They also classified bots based on the content posted, time before the bot gets suspended, and type of activity the bot does (tweet or retweet) into the following categories:

1. Core Bots: These bots are further divided into three sub-categories:
   (a) Generator Bots: bots that tweet a lot but seldom retweet anything.
   (b) Short Lived Bots: bots that retweet a lot but seldom tweet. These bot accounts lasted around 6 weeks before Twitter suspended them.
   (c) Long Lived Bots: bots that retweet a lot but seldom tweet. These bot accounts lasted more than 25 weeks before Twitter suspended them.
2. Peripheral Bots: Twitter accounts that are being lured to participate in the dissemination process. Their task is retweeting one or more tweets generated by the core bots [15].

Research on detecting social bots has increased dramatically. In 2010, Chu et al. [17] proposed a classification system to determine whether tweets on Twitter belong to a human, bot, or cyborg (human account use scripts or tools to post on their

behalf, like a hybrid account). Over 500,000 accounts were studied to find the difference between human, bots, and cyborg in tweeting content and behavior. Their classifier is comprised of the following four components: (1) Entropy Component: which is used to detect the regularity and periods of users' tweets, (2) Machine Learning Component: which is used to detect spam tweets, (3) Account Properties Component: which help identify bots by checking external URLs ratio in the tweets or checking the tweeting device (web, mobile, or API) to help detecting bots, and (4) Decision Maker Component: which uses the input of the previous three components to determine the type of the user [17].

Wang et al. [18] reviewed the possibility of human detection, suggesting the crowdsourcing of social bot detection to legions of workers. To test this concept, the authors created an Online Social Turing Test platform. The authors assumed that bot detection is a simple task for humans because humans have a natural ability to evaluate conversational nuances like sarcasm or persuasive language and to observe emerging patterns or anomalies but this is yet unparalleled by machines. Using data from Facebook and Renren—a popular Chinese online social network—the authors tested the efficacy of humans—both expert annotators and workers hired online—at detecting social bot accounts simply from the information on their profiles. The authors observed the detection rate for hired workers drops off over time, although it remains good enough to be used in a majority voting protocol. In their experiment, the same profile was shown to multiple workers and the opinion of the majority was used to determine the final verdict.

The derivative of this literature identifies that bots are present in the current information environment. Sophisticated studies indicate that bots are difficult to monitor even as researchers develop advanced detection methods. Bots are continually growing more advanced demonstrating more human-like behavior [19] which makes them harder to detect, especially if they start to inject "bot" opinions into messaging. Findings from the DARPA "Twitter Bot Detection Challenge" show that bots cannot be solely identified using machine learning only, instead a vast enhancement of analytic tools that combine multiple approaches to help in bot detection is needed [20]. Hence in this chapter, we combine SNA and SCF to help in bot identification, especially in dark networks.

Social Cyber Forensics (SCF) For the last three and half decades digital forensics tools have evolved from simple tools, which were used mainly by law enforcement agencies to import tools for detecting and solving corporate fraud [21]. Cyber forensics tools are not new but they are evolving over time to have more capabilities, more exposure to the audience (investigators or public users), and more types and amount of data that can be obtained using each tool. Cyber forensics tools can be traced back to the early 1980s 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 or C language with limited capabilities and less popularity. With time these tools got more sophisticated and in the mid of 1980s these tools were able to recognize file types as well as retrieve lost or deleted files, e.g., XtreeGold and DiskEdit by Norton. In 1990s these

tools became 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 [22]. Nowadays, many tools are available to the public that enable them to collect cyber forensics data and visualize it in an easy to understand way, e.g., Maltego tool (developed by Paterva Ltd. available at www.paterva.com).

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, or 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) [23].

Research by Noora et al. [24] 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 [24]. Additional research focused on extracting forensics data of social media from the computer hard disk such as carving artifacts left by the use of Facebook Chat on a computer's hard disk [25].

In this work, we are not creating a tool to collect forensics data from social networks, instead we are using a social cyber forensic analysis tool called Maltego which collects open source information (OSINF) and forensics data. This tool provides a library of transformations for 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, LinkedIn, and Twitter. It also provides the capability to visualize the results in a graph format that is suitable for link analysis.

Social Network Analysis Borgatti implies that the importance of an organization in a given network is determined by the institutional affiliations it has within the network [7]. The flow of information amongst the institutional affiliates will illuminate areas that are not identified without the use of exploratory social network analysis. Often these networks are referred to as *dark networks*. SNA should aid in the overall strategy to identify kinetic and non-kinetic operations, but should not be the definitive component of a stratagem. Applying SNA combined with SCF allows for network illumination of the dark networks.

Common centrality measures such as betweenness, eigenvector, and closeness are used throughout this research. Although these metrics are primary in this research, other areas of SNA are examined as well such as topography, cohesive subgroups, components, and Focal Structure Analysis (FSA).

Networks that portray the shortest paths between the organizations inside of the network, demonstrate betweenness centrality. Further defined, nodes with the closest neighbors are measured by their betweenness centrality [26]. These

network measurements are seen in several of the sociograms throughout the chapter. Eigenvector centrality was used to illuminate hierarchy within the organizations. This will display well-connected nodal connections to other well connected nodes [27]. Closeness centrality allows this research to identify the dissemination of information throughout the network. It is imperative to not use closeness as a stand alone metric "This could lead analysts to conclude that certain actors are more important than they really are which of course could lead to using mistaken assumptions when crafting strategies " [28]. It is not unusual that illumination of higher level actors are already common knowledge to the public. Often, bots are used to amplify the messages. Because of the truly hidden ways that bots have been disguised it was necessary to combine SNA and SCF to illuminate the bots.

Focal Structure is an algorithm that was implemented by Şen et al. [29] to discover an influential group of individuals in a large network. FSA is not a community detection algorithm, i.e., in the context of networks, most community detections algorithms try to find nodes that are more densely connected in one part of the network and not that much connected on the other part of the network. These community detection algorithms would suggest that there is a community based on the nodes connection strength (i.e., how closely they are connected). However, FSA is an algorithm that tries to find a key set of nodes that are influential if they are working together (i.e., exist in the network whether they are directly connected or not). These individuals need not to be strongly connected and may not be the most influential actors on their own, but by acting together they form a compelling power.

FSA is a recursive modularity-based algorithm. Modularity is a network structural measure that evaluates the cohesiveness of a network [30]. FSA uses a network-partitioning approach to identify sub-structures or sub-graphs. FSA consists of two parts the first part is a top-down division, where the algorithm identifies the candidate focal structures in the complex network by applying the Louvain method of computing modularity [31]. The second part is a bottom-up agglomeration, where the algorithm stitches the candidate focal structures, i.e., the highly interconnected focal structures, or the focal structures that have the highest similarity values, are stitched together and then the process iterates until the highest similarity of all sibling pairs is less than a given threshold value. Similarity between two structures is measured using Jaccard's Coefficient [29, 32] which results in a value between 0 and 1, where 1 means the two networks are identical, while zero means the two networks are not similar at all. The stitching of the candidate focal structures was done to extract the structures with low densities, i.e., structures contain nodes that are not connected densely [29].

Influence in Blogosphere Blogs provide rich medium for individuals to frame an agenda and develop discourse around it using half-truth or twisting facts to influence the masses. Twitter, however, due to the 280-character limit, is primarily used as a dissemination medium. Bloggers have used Twitter to build an audience (or, followership) 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 is a well-studied problem. Many studies have been conducted to identify the influence of a blogger in a community [33–37]. The basic idea of computing the influence a blogger has is to aggregate the influence of their individual blog posts. A blog post having more *in-links* and *comments* indicates that the community is interested in it. *In-links* and *comments* contribute *positively* towards the influence of the posts whereas *out-links* of the blog posts contribute *negatively* towards the influence. Influence can be assessed using a stochastic model with *inbound links*, *comments* and *outbound links* of a post as factors, as proposed in [33]. An alternate approach is to use a modification of *Google page rank* to identify influential posts as well as bloggers [36].

3 Methodology to Study Narratives and Propaganda

In this section, we provide a methodology to study narratives including propaganda that is disseminated on various social media channels during various events. This methodology has been tested on several case studies and provided consistent results. The overall methodology is depicted in Fig. 1. The methodology first starts by domain experts identifying keywords relevant to an event. Second, searching various online social media platforms is conducted to identify an initial seed of data, e.g., Twitter accounts tweeting propaganda about the event, or a YouTube video containing propaganda, or a blog site that contain narratives. Third, using various data collection tools (NodeXL, Scraawl, Web Crawlers (e.g., WebContentExtracor), YouTube APIs, Twitter APIs, TAGs, and Maltego) we extracted the social and communication networks of Twitter users, crawled the blog's data, identified bots, and extracted the metadata associated with the social media accounts of interest. Finally, we conducted a set of analyses on the collected data including:

- Social Cyber Forensics (SCF) analysis to identify relations among various groups, uncover their cross-media affiliation, and identify more groups.
- Social Network Analysis (SNA) to identify leaders of the narrative and identify the role of nodes in the network, e.g., the source of information, brokers, top disseminators, and type of nodes (bot or human account).
- We also conduct various blogs data analyses using our in-house developed Blogtrackers tool (available at: http://blogtrackers.host.ualr.edu) such as sentiment analysis, keywords trends, influential blogs and bloggers, etc.

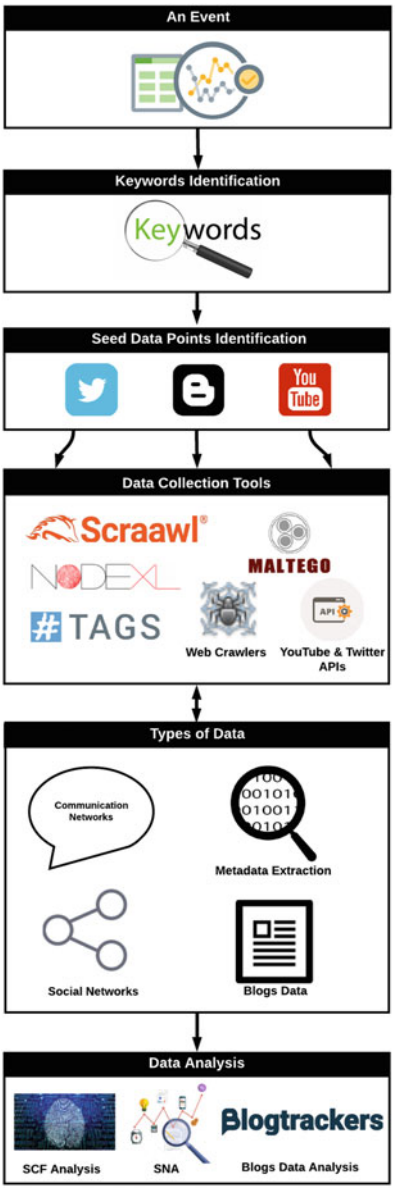

Fig. 1 The overall research methodology

3.1 Case Study 1: Anti-NATO Propaganda During the 2015 Trident Juncture Exercise

What Was the Propaganda On 4 November 2015, the US soldiers along with soldiers from more than thirty partner nations and Allies moved 36,000 personnel across Europe during the 2015 Trident Juncture Exercise (TRJE). The exercise took place in the Netherlands, Belgium, Norway, Germany, Spain, Portugal, Italy, the Mediterranean Sea, the Atlantic Ocean, and also in Canada to prove the capability and readiness of the Alliance on land, air, and maritime. The exercise also demonstrated that the Alliance is equipped with the appropriate capabilities and capacities to face any present or future security issues. In addition to the Partner Nations and Allies, more than Twelve aid agencies, International Organizations, and non-governmental organizations participated in the exercise to demonstrate "NATO's commitment and contribution to a comprehensive approach [38]."

The buildup of the exercise saw a series of competing information maneuvers designed to counter NATO and Allies. Several of these maneuvers are highlighted as examples that were observed in Fig. 2 below. Ranging from narrative hijacking in multiple languages across websites, to community counter NATO meetings, to protests in the streets, and of note an Anti-NATO concert held in Zaragoza. All of which were pushed via social platforms months before the exercise and created a information deficit that NATO had to fill.

Many opponent groups launched campaigns on Twitter, Blogs, Facebook, and other social media platforms that encouraged citizens to protest against the exercise

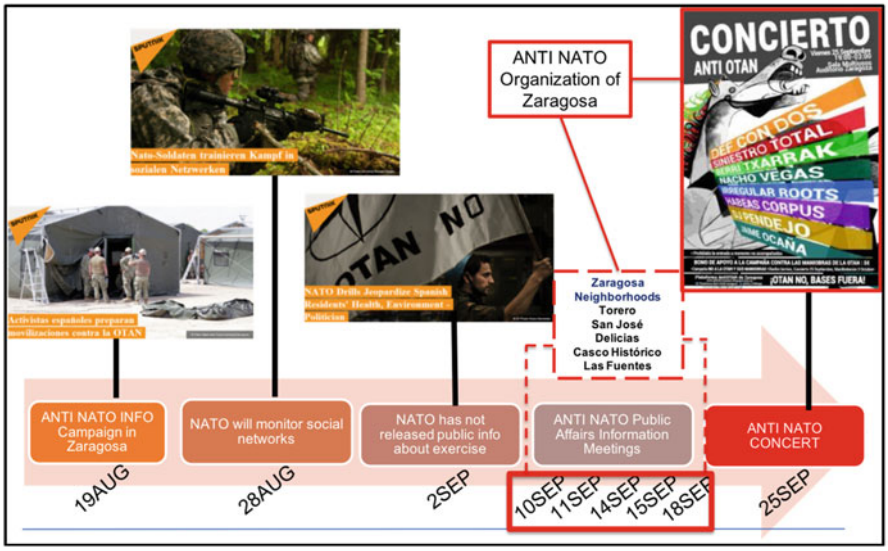

Fig. 2 Examples of Anti NATO activities that were observed in the information environment prior to the exercise [39–41]

or do violent acts. We identified six groups by searching their names on various social media platforms to identify their Twitter and blogging profiles (followed our proposed methodology). These six groups propagated their messages on social media inviting people to act against NATO and TRJE 2015 exercise. Next, we provide a description of the dataset along with our findings.

Data Collection 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, 1365 mentions, 9129 total nodes, and 10,824 total edges. The twitter handles, blogs, and names of the groups studied in this research are publicly available. However, in order to ensure their privacy, we do not disclose them here.

Metadata Extraction We used Maltego which 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 [42]. Using this identifier other blog sites that are managed under the same UA number can be identified. This method was reported in Bazzell's Open Source Intelligence Techniques: Resources for searching and analyzing online information [43]. Using Maltego we inferred the connections among blog sites and identified 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 the tool in a snowball manner to discover other blog sites. We were able to identify additional 9 blogs that were 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* [44]. Additional public information such as the IP addresses, website owner name, email address, phone numbers, and locations of all the websites was reviewed. 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 the 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 is stored in a database that the Blogtrackers tool can access and analyze.

Identifying Influential Information Actors Using SNA In addition to extracting metadata using Maltego to find other related blog sites used by the group to disseminate their propaganda, we applied SNA such as indegree centrality (to assess popular nodes) outdegree centrality (to assess information sources or gregarious nodes), betweenness centrality (to assess information brokers or bridges) to find the most important nodes in the network by activity type we also applied various community detection measures such as modularity (to assess the quality of the clusters), etc. Using NodeXL we were able to find the most used hashtags during the time of the exercise (i.e., the hashtags occurred the most in the collected tweets). 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. 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.

Identifying Powerful Groups of Individuals Affecting Cyber Propaganda Campaign using FSA We divided our network (9129 nodes and 10,824 unique edges) into two type 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.

Analyzing Blogs Data Using Blogtrackers 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. Then we performed the following analysis:

1. We explore the collected dataset by generating the traffic pattern graph using Blogtrackers. We ran the analysis 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. We generated a keyword trends graph for the following keywords: 'anti nato', 'trident juncture', 'nato' (as shown in Fig. 3). 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 wanted to identify what resonates with the community most, or which narratives are affecting the people most. The influence score was calculated using of a stochastic model [33] with *inbound links*, *comments* and *outbound links* of a post as factors. The most influential

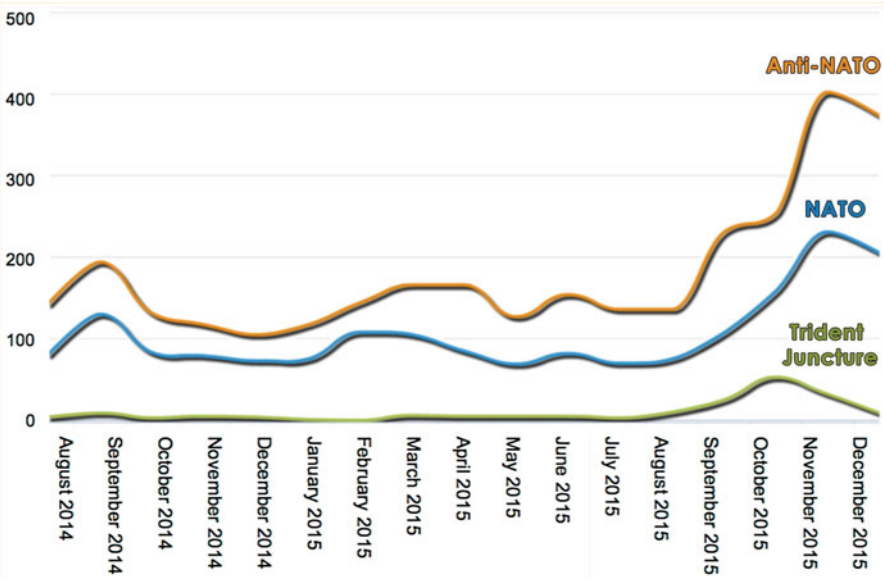

Fig. 3 Keyword trends for "anti nato," "nato," and "trident juncture" generated by Blogtrackers depicting the occurrence of these keywords over the time period

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 [45] 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.

3.2 Case Study 2: Anti-NATO Propaganda During the 2015 Dragoon Ride Exercise

What Was the Propaganda On 21 March 2015, US soldiers assigned to the 3rd Squadron, 2nd Cavalry Regiment in Estonia, Latvia, Lithuania, and Poland as part of Operation Atlantic Resolve began Operation Dragoon Ride. US troops, nicknamed 'Dragoons', initiated a military movement which stretched from the Baltics to Germany, crossing five international borders and covering more than 1100 miles. This mission exercised the unit's maintenance and leadership capabilities and also demonstrated the freedom of movement that exists within NATO [46].

Many opponent groups launched campaigns to protest the exercise, e.g., 'Tanks No Thanks' [47], which appeared on Facebook and other social media sites, promising large and numerous demonstrations against the US convoy [48]. Czech President Milos Zeman expressed sympathy with Russia; his statements were echoed in the pro- Russian English language media and the Kremlin financed media, i.e., Sputnik news [49]. The RT website also reported that the Czechs were not happy with the procession of the "U.S.Army hardware" [47]. However, thousands of people from the Czech Republic welcomed the US convoy as it passed through their towns, waving US and NATO flags, while the protesters were not seen.

During that time many bots were disseminating propaganda, asking people to protest and conduct violent acts against the US convoy. A group of these bots was identified using Scraawl (available at www.scraawl.com), an online social media analysis product developed for bot detection and discourse analysis. It's an easy-to-use discovery tool of Intelligent Automation, Inc. for open source information. The link will provide you a free test subscription, if you'd like to try it out yourself. We collected data on this network of bots and studied its structure in an attempt to understand how they operated. Next, we provide a description of the dataset and our findings.

Data Collection We collected data for the period between 8 May 2015 and 3 June 2015 of 90 Twitter accounts that were identified by Scraawl as bots known to disseminate propaganda during the Dragoon Ride Exercise. Out of the 90 Twitter accounts we were able to collect data from 73 accounts. We were not able to collect

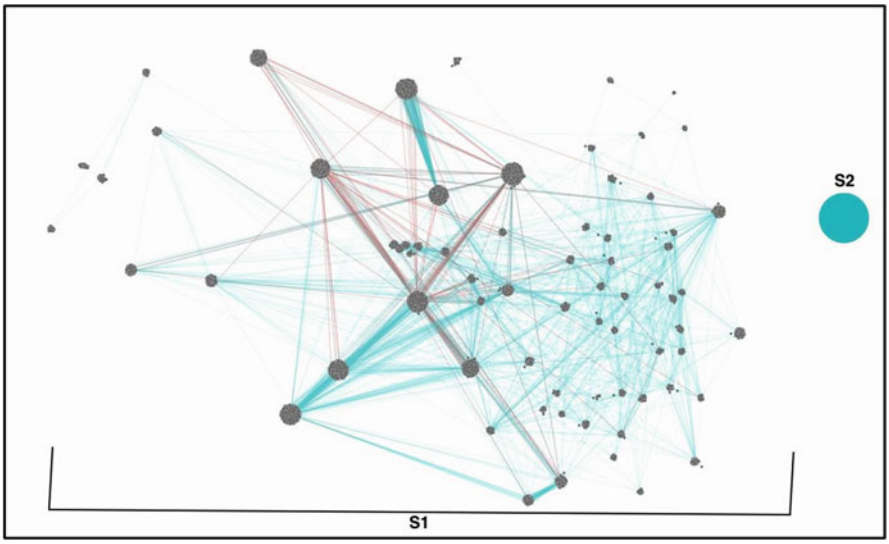

Fig. 4 Two sub-networks, S1 and S2. S1 is un-collapsed while S2 is collapsed. Edges in blue denote mutually reciprocal relations (bidirectional edges) while edges in red color denote non-reciprocal relations (unidirectional edges)

data for 17 Twitter accounts because the accounts had been either *suspended, did not exist*, or were *set to private*. Data was collected using NodeXL—an excel plugin for social media data collection and analysis— that included: friend and follower relations, tweet, mention, and reply relations. This resulted in 24,446 unique nodes and 31,352 unique edges. An 'edge' is a 'relationship', which can be a tweet, retweet, mention, reply, or friendship between two nodes (Twitter accounts). We obtained 50,058 non-unique edges with 35,197 friends and followers edges, 14,428 tweet edges, 358 mention edges, and 75 reply edges.

Analysis of Case Study 2 We analyzed the friend/follower networks (social network) of the bot accounts. We applied the Girvan-Newman clustering algorithm [30] to this network and found that the network had two clusters, S1 and S2, as shown in Fig. 4.

The clusters are the same as the components in this graph. The smaller S2 cluster, containing only a triad of nodes, was rejected from further analysis, as it did not contribute much to the information diffusion. Since the larger S1 cluster contained the majority of nodes, we examined this sub-network further.

Zooming in for a closer examination of the S1 cluster revealed that the members of that network were more akin to a syndicate network, i.e., a network that has dense connections among their members and inter-group connections with the other nodes and do not have a most central node, i.e., no hierarchy. Further examination of the nodes in S1 revealed a mutually reciprocated relationship (the nodes followed each other), suggesting that the principles of '*Follow Me and I Follow You'*

(FMIFY) and 'I Follow You, Follow Me' (IFYFM)—a well-known practice used by Twitter spammers for 'link farming', or quickly gaining followers [50, 51] were in practice—a behavior that was also observed during other study we conducted on the Crimean Water Crisis botnet [52, 53].

This network had no central node or no start-shaped network. In other words, there was no single node feeding information to the other bots, or seeder of information (this was determined using indegree centrality measure). This indicated the absence of a hierarchical organizational structure in the S1 network, in other words no seeder was identified/observed. In cases where the seeder is not easily identifiable, other, more sophisticated methods are warranted to verify if this behaviour truly does not exist. Although there might not be a single most influential node, a group of bots may be coordinating to make an influential group. To study this behaviour further, we applied the Focal Structures Analysis (FSA) approach to find if any influential group of bots existed [54].

FSA has been tested on many real world cases such as the Saudi Arabian Women's Right to Drive campaign on Twitter [55] and the 2014 Ukraine Crisis when President Viktor Yanukovych rejected a deal for greater integration with the European Union and three big events followed—Yanukovych was run out of the country in February, Russia invaded and annexed Crimea in March, and pro-Russian separatist rebels in eastern Ukraine brought the relationship between Russia and the West to its lowest point since the Cold War. Applying focal structures during the two aforementioned examples revealed interesting findings. It was proven that during the Saudi Arabian Women's Right to Drive Twitter campaign on 26 October 2013 the focal structures were more interactive than average individuals in the evolution of a mass protest, i.e., the interaction rate of the focal structures was significantly higher than the average interaction rate of random sets of individuals. It was also proven that focal structures were more interactive than communities in the evolution of a mass protest, i.e., the number of retweets, mentions, and replies increases proportionally with respect to the followers of the individuals in communities [29]. Applying the FSA approach to the Ukraine-Russia conflict also revealed an interesting finding. By applying FSA to a blog-to-blog network, Graham W. Phillips [56]—a 39-year-old British journalist and blogger—was found to be involved in the only focal structure of the entire network along with ITAR-TASS, the Russian News Agency, and Voice of Russia, the Russian government's international radio broadcasting service. Even though other central and well-known news sources, such as the Washington Post and The Guardian, were covering the events, Phillips was actively involved in the crisis as a blogger and maintained a single-author blog with huge influence that compared with some of the active mainstream media blogs. Phillips covered the 2014 Ukraine crisis and became a growing star on Kremlin-owned media. He set out to investigate in a way that made him a cult micro-celebrity during the crisis—by interviewing angry people on the street for 90 s at a time [57].

While the bot detection methodology used in this study is not 100% accurate, we used tools that are commonly used by government agencies. A manual check of accounts identified as bots by the tools used served as an additional verification.

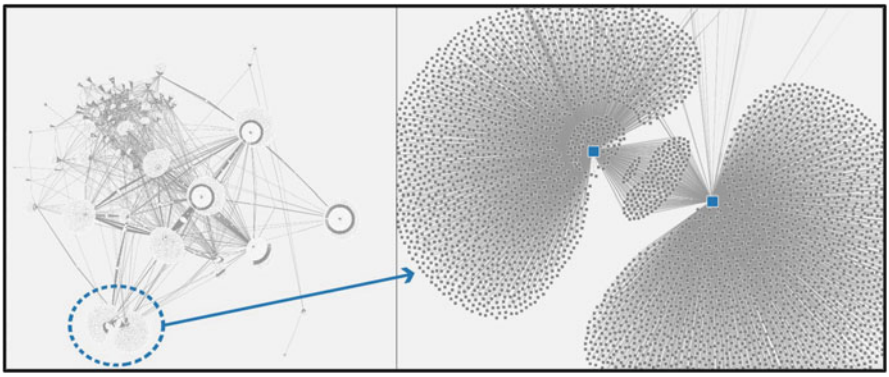

Fig. 5 The social network (friends/followers network) of the botnets. The focal structure analysis approach helped in identifying a highly sophisticated coordinating structure, which is marked inside the blue circle in the figure on left. Upon zooming-in on this structure (displayed on the right), two bots were identified as the seeders in this focal structure. The seeder bots are depicted in blue

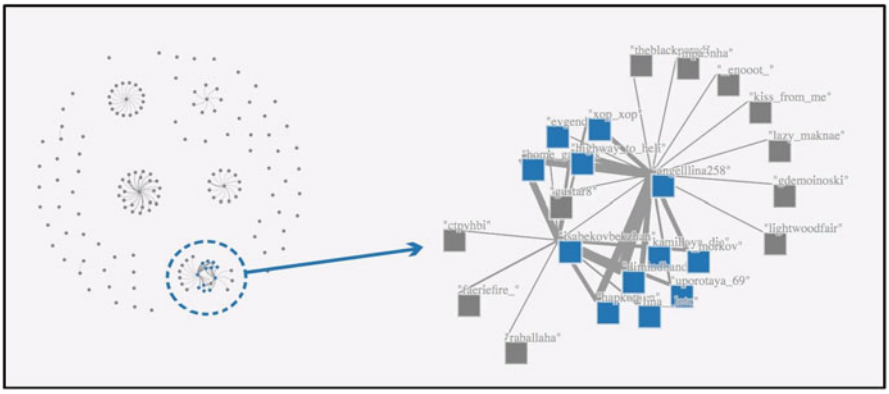

Fig. 6 Communication network (tweets, mentions, and replies network) of the botnets. Ten nodes were communicating the most with the two most influential bots in the network

We ran the FSA approach on the Dragoon Ride data to discover the most influential set of bots or the seeders of information in the S1 community. By applying FSA to the social network of these bots we obtained one focal structure containing two nodes (see Fig. 5). These two nodes form the most influential set of bots in the network, i.e., by working together those two bots had a profound impact on the dissemination of propaganda.

We further applied FSA to the bots' communication network, i.e., tweets, mentions, and replies network to identify who are the most communicative nodes in this network (see Fig. 6). We obtained one focal structure containing 12 nodes. Ten nodes were 'real people nodes', i.e., nodes that communicated the most with bots

(potential seeders of information), while the other two nodes were the bots identified as the most influential nodes in the friends and followers network.

In this case study, deviant groups used a sophisticated tool to disseminate their propaganda and speed up the dissemination process by using botnets. These botnets were very sophisticated compared to a study we previously conducted on the use of social bots during the Crimean water crisis in 2014 [52, 53]. The network structure of the botnets in the latter case is much more complex than in the former. Botnets in the Dragoon Ride exercise case required a more sophisticated approach to identify the organizers or seeders of information, i.e., it required applying FSA to both the social network (friends/followers network) and the communication network (tweets, replies, and mentions network). The evolution of complexity in the bots' network structures confirms the need for a systematic study of botnet behavior to develop sophisticated approaches/techniques or tools that can deal with predictive modelling of botnets.

4 Conclusion

In conclusion, the rapid advancement of technology has made people more connected than ever before. Internet, especially social media, has enabled the flow of information at unprecedented rates. This amplification is observed more in the spread of misinformation, fake or inaccurate news, and propaganda. Conducting deviant acts has become more convenient, effective, and rapid. Deviant groups can coordinate cyber campaigns in order to achieve strategic goals, influence mass thinking, and steer behaviors or perspectives about an event in a highly coordinated and sophisticated manner that remains largely undetected.

In this chapter, we provided two important and detailed case studies, namely the NATO's 2015 Trident Juncture Exercise (TRJE 2015) and 2015 Dragoon Ride Exercise. We study the online deviant groups (ODGs) and their behavior in conducting deviant acts, especially disseminating propaganda against NATO during the two exercises. We analyzed situational awareness of the real-world information environment in/around those events by employing computational social network analysis and social cyber forensics informed methodologies. These methodologies help identify information competitors who seek to take the initiative and the strategic message away from the main event in order to further their own agenda. We describe our methodology, analysis (node-level, group-level analysis, and content-level), and results obtained in both case studies. We further study how ODGs use social media in coordinating cyber propaganda campaigns. The research offered many interesting findings and were of great benefit to NATO and U.S. forces participating in both exercises on the ground.

Acknowledgment This research is funded in part by the U.S. National Science Foundation (IIS-1636933, ACI-1429160, and IIS-1110868), U.S. Office of Naval Research (N00014-10-1-0091, N00014-14-1-0489, N00014-15-P-1187, N00014-16-1-2016, N00014-16-1-2412, N00014-17-1-2605, N00014-17-1-2675), 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), the Jerry L. Maulden/Entergy Fund at the University of Arkansas at Little Rock, the Arkansas Research Alliance, and Creighton University's College of Arts and Sciences. 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. Professor describes Atari's impact on gaming world. Technique, http://nique.net/life/2009/02/20/professor-describes-ataris-impact-on-gaming-world/. Accessed 1 May 2018
2. M. Zuckerberg, Biography.com, https://www.biography.com/people/mark-zuckerberg-507402. Accessed 3 May 2018
3. C. Gallo, Jeff Bezos banned powerpoint in meetings. His replacement is brilliant. Inc.com (2018), https://www.inc.com/carmine-gallo/jeff-bezos-bans-powerpoint-in-meetings-his-replacement-is-brilliant.html. Accessed 28 Apr 2018
4. D. Volkov, Supporting a war that isn't: Russian public opinion and the Ukraine conflict. Carnegie Moscow Center (2015), https://carnegie.ru/commentary/61236. Accessed 9 Jan 2019
5. D.V. Gioe, Cyber operations and useful fools: the approach of Russian hybrid intelligence. Intell. Natl. Secur. **33**, 954–973 (2018). https://doi.org/10.1080/02684527.2018.1479345
6. S. Tatham, *Strategic Communication: A Primer* (Defence Academy of the United Kingdom, Conflict Studies Research Centre, Camberley, 2008)
7. S.P. Borgatti, Centrality and network flow. Soc. Networks **27**, 55–71 (2005). https://doi.org/10.1016/j.socnet.2004.11.008
8. M.K. Sparrow, The application of network analysis to criminal intelligence: an assessment of the prospects. Soc. Networks **13**, 251–274 (1991). https://doi.org/10.1016/0378-8733(91)90008-h
9. R.B. Cialdini, *Influence: Psychology of Persuasion* (Collins Business, New York, 1993)
10. Senior Research Psychologist – Connections, amazon.jobs, https://www.amazon.jobs/en/jobs/655074/senior-research-psychologist-connections. Accessed 20 May 2018
11. R.A. Rodríguez-Gómez, G. Maciá-Fernández, P. García-Teodoro, Survey and taxonomy of botnet research through life-cycle. ACM Comput. Surv. **45**, 1–33 (2013). https://doi.org/10.1145/2501654.2501659
12. M.S. Ackerman, J. Muramatsu, D.W. Mcdonald, Social regulation in an online game, in *Proceedings of the 16th ACM International Conference on Supporting Group Work - GROUP 10* (2010). https://doi.org/10.1145/1880071.1880101
13. S. Hegelich, D. Janetzko, Are social bots on Twitter political actors? Empirical evidence from a Ukrainian social botnet, in *Proceedings of the Tenth International AAAI Conference on Web and Social Media (International AAAI Conference on Web and Social Media (ICWSM-16)* (2016)
14. A. Karasaridis, B. Rexroad, D. Hoeflin, Wide-scale botnet detection and characterization, in *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets (HotBots'07)* (USENIX Association, Berkeley, CA, 2007), p. 7-7
15. N. Abokhodair et al., Dissecting a social botnet: growth, content and influence in Twitter, in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, CSCW '15*, ed. by D. Cosley et al. (ACM, New York, 2015), pp. 839–851

16. S. Al-khateeb, N. Agarwal, Examining botnet behaviors for propaganda dissemination: a case study of ISIL's beheading videos-based propaganda, in *Proceedings of the Behavior Analysis, Modeling, and Steering (BEAMS 2015) co-located with the IEEE International Conference on Data Mining (ICDM 2015)* (2015)
17. Z. Chu et al., Who is tweeting on Twitter: human, bot, or cyborg? in *Conference, 2010 Annual Computer Security Applications Conference (ACSAC 2010), Austin, TX, USA - December 06 - 10, 2010* (ACM, New York, 2010), pp. 21–30
18. G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng, B.Y. Zhao, Social turing tests: crowdsourcing sybil detection, in *The Network and Distributed System Security Symposium (NDSS)* (The Internet Society, 2013)
19. E. Ferrara, O. Varol, C. Davis, et al., The rise of social bots. Commun. ACM **59**, 96–104 (2016). https://doi.org/10.1145/2818717
20. V. Subrahmanian, A. Azaria, S. Durst, et al., The DARPA Twitter bot challenge. Computer **49**, 38–46 (2016). https://doi.org/10.1109/mc.2016.183
21. N. Alherbawi, Z. Shukur, R. Sulaiman, Systematic literature review on data carving in digital forensic. Procedia Technol. **11**, 86–92 (2013). https://doi.org/10.1016/j.protcy.2013.12.165
22. K. Oyeusi, *Computer Forensics* (London Metropolitan University, London, 2009)
23. M. Mulazzani, M. Huber, E. Weippl, Social network forensics: tapping the data pool of social networks, in *Eighth Annual IFIP WG*, vol. 11 (2012)
24. N.A. Mutawa, I. Baggili, A. Marrington, Forensic analysis of social networking applications on mobile devices. Digit. Investig. **9**, S24 (2012). https://doi.org/10.1016/j.diin.2012.05.007
25. N.A. Mutawa, I.A. Awadhi, I.M. Baggili, A. Marrington, Forensic artifacts of Facebook's instant messaging service, in *2011 International Conference for Internet Technology and Secured Transactions* (2011), pp. 771–776
26. K.M. Carley, J. Reminga, ORA: organization risk analyzer. Technical Report, Carnegie Mellon University, School of Computer Science, Institute for Software Research International (2004), http://www.casos.cs.cmu.edu/publications/papers/carley_2004_oraorganizationrisk.pdf. Accessed 21 May 2018
27. G. Cheliotis, Social network analysis. LinkedIn SlideShare (2010), https://www.slideshare.net/gcheliotis/social-network-analysis-3273045. Accessed 25 May 2018
28. S.F. Everton, Strategic options for disrupting dark networks, in *Disrupting Dark Networks*, (Cambridge University Press, New York, 2012), pp. 32–46. https://doi.org/10.1017/cbo9781139136877.004
29. F. Şen, R. Wigand, N. Agarwal, et al., Focal structures analysis: identifying influential sets of individuals in a social network. Soc. Netw. Anal. Min. **6**, 17 (2016). https://doi.org/10.1007/s13278-016-0319-z
30. M. Girvan, M.E.J. Newman, Community structure in social and biological networks. PNAS **99**(12), 7821–7826 (2002)
31. V.D. Blondel, J.-L. Guillaume, R. Lambiotte, E. Lefebvre, Fast unfolding of communities in large networks. J. Stat. Mech: Theory Exp. **2008**, P10008 (2008). https://doi.org/10.1088/1742-5468/2008/10/p10008
32. P. Jaccard, The distribution of the flora in the alpine zone. New Phytol. **11**(2), 37–50 (1912)
33. N. Agarwal, H. Liu, L. Tang, P.S. Yu, Identifying the influential bloggers in a community, in *Proceedings of the International Conference on Web Search and Web Data Mining - WSDM 08* (2008). https://doi.org/10.1145/1341531.1341559
34. N. Agarwal et al., Modeling blogger influence in a community. Soc. Netw. Anal. Min. **2**(2), 139–162 (2012)
35. S. Kumar et al., Convergence of influential bloggers for topic discovery in the blogosphere, in *International Conference on Social Computing, Behavioral Modeling, and Prediction*, ed. by S.-K. Chai et al. (Springer, Berlin 2010), pp. 406–412
36. A. Java, P. Kolari, T. Finin, T. Oates, Modeling the spread of influence on the blogosphere, in *Proceedings of the 15th International World Wide Web Conference* (2006), pp. 22–26

37. 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)
38. A.J. Girao, Tried and tested, in *NATO Summit 2016 – Strengthening Peace and Security* (2016), pp. 105–107
39. Sputnik, Activistas españoles preparan movilizaciones contra la OTAN. Sputnik Mundo (2015), http://mundo.sputniknews.com/espana/20150819/1040501131.html. Accessed 20 Aug 2015
40. Sputnik, Nato-Soldaten trainieren Kampf in sozialen Netzwerken. Sputnik Deutschland (2015), http://de.sputniknews.com/militar/20150828/304057978.html. Accessed 2 Sep 2015
41. Sputnik, NATO drills jeopardize Spanish residents' health, environment - politician. Sputnik International (2015), http://sputniknews.com/military/20150902/1026475239/nato-drills-zaragoza.html. Accessed 2 Sep 2015
42. L. Alexander, Open-source information reveals pro-kremlin web campaign. Global Voices (2015), https://globalvoices.org/2015/07/13/open-source-information-reveals-pro-kremlin-web-campaign. Accessed 21 May 2018
43. M. Bazzell, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information* (Createspace Independent Publishing, Charleston, 2016)
44. B. Etling, J. Kelly, R. Faris, J. Palfrey, *Mapping the Arabic blogosphere: politics, culture, and dissent*, vol 6 (Berkman Center for Internet & Society, Cambridge, 2009)
45. R.B. Standler, Propaganda and how to recognize it (RBS0), www.rbs0.com/propaganda.pdf. Accessed 2 Sep 2005
46. Operation Atlantic Resolve Exercises Begin in Eastern Europe. U.S. Department of Defense. https://www.defense.gov/News/Article/Article/604341/operation-atlantic-resolve-exercises-begin-in-eastern-europe/. Accessed 21 May 2018
47. 'Tanks? No thanks!': Czechs unhappy about US military convoy crossing country. RT International. https://www.rt.com/news/243073-czech-protest-us-tanks/. Accessed 21 May 2018
48. D. Sindelar, U.S. Convoy, in Czech Republic, Real-Life Supporters Outnumber Virtual Opponents, Radio Free Europe/Radio Liberty (2015)
49. Sputnik, Czechs plan multiple protests of US Army's 'operation dragoon ride'. Sputnik International (2015), https://sputniknews.com/europe/201503281020135278/. Accessed 21 May 2018
50. S. Ghosh, B. Viswanath, F. Kooti, et al., Understanding and combating link farming in the twitter social network, in *Proceedings of the 21st international conference on World Wide Web - WWW 12* (2012). https://doi.org/10.1145/2187836.2187846
51. V. Labatut, N. Dugue, A. Perez, Identifying the community roles of social capitalists in the Twitter network, in *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)* (2014). https://doi.org/10.1109/asonam.2014.6921612
52. S. Al-Khateeb, 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. **2**, 6 (2016). https://doi.org/10.1515/jobs-2016-0028
53. N. Agarwal, S. Al-Khateeb, R. Galeano, R. Goolsby, Examining the use of botnets and their evolution in propaganda dissemination. Def. Strateg. Commun. **2**, 87–112 (2017). https://doi.org/10.30966/2018.riga.2.4
54. Şen F, Wigand R, Agarwal N, et al., Focal Structure Analysis in Large Biological Networks, in *IPCBEE (2014 3rd International Conference on Environment Energy and Biotechnology)*, vol. 70 (IACSIT Press, Singapore, 2014), p. 1
55. S. Yuce et al., Studying the evolution of online collective action: Saudi Arabian Women's "Oct26Driving" Twitter campaign, in *International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction*, ed. by W.G. Kennedy et al. (Springer, Cham, 2014), pp. 413–420

56. Graham Phillips is a British national contracted as a stringer by the Russian Times (RT). He has produced numerous videos, blogs, and stories in and around eastern Ukraine. He speaks and writes in Russian and English in his reports. He recently spent time covering the World Cup in Brazil for RT and has re-entered Eastern Ukraine as of July 2014. RT reported on that Phillips was deported from Ukraine because he works for RT. He will not be allowed to re-enter Ukraine for three years.
57. M. Seddon, How a British blogger became an unlikely star of the Ukraine conflict - and Russia Today. BuzzFeed, https://www.buzzfeed.com/maxseddon/how-a-british-blogger-became-an-unlikely-star-of-the-ukraine?utm_term=.poaNaBd7w#.ikzWz90Ny. Accessed 21 May 2018