Volume 2 | Spring 2017

DEFENCE STRATEGIC COMMUNICATIONS

The official journal of the NATO Strategic Communications Centre of Excellence

EXAMINING THE USE OF BOTNETS AND THEIR EVOLUTION IN PROPAGANDA DISSEMINATION

Nitin Agarwal, Samer Al-khateeb, Rick Galeano, Rebecca Goolsby

Abstract

Social media is increasingly used to communicate strategic information during crises and to enable authorities to act tactfully. Numerous journalistic accounts have highlighted the prolific and disturbing use of social media by deviant groups among state and non-state actors to influence public opinion and provoke hysteria among citizens through disseminating misinformation or propaganda about various influential events such as the 2014 Crimean Water Crisis or the 2015 Dragoon Ride Exercise. We study the strategic communication used by deviant groups within the social media ecosystem, especially examining the cross-influence between blogs and Twitter. We have collected and analysed data from blogs and Twitter during the two aforementioned events. Our study shows that networked computers running automated and coordinated programs to perform specific tasks, or 'botnets' have been extensively used during the two events, greatly increasing the dissemination of propaganda. Furthermore, the behaviours of these botnets are becoming increasingly sophisticated over time, both from the perspective of information dissemination as well as coordination. The evolving behaviours of botnets make them elusive, even to state-of-the-art detection techniques, warranting more sophisticated botnet detection methodologies. In this study, we present methodologies informed by social science and computational network analysis to study the information dissemination and coordination behaviours of botnets and to aid the development of detection tools ready for deployment in cyber operations.

Keywords: information warfare, cyber operations, social media, Twitter, blogs, strategic communications, botnets, propaganda, disinformation campaigns, social network analysis, focal structures.

About the authors

Samer Al-khateeb is a PhD student at the University of Arkansas. He majors in Computer and Information Sciences with research interest in deviant behavioural modeling, deviant cyber flash mobs, cyber propaganda campaigns, and social cyber forensics.

Nitin Agarwal is the Jerry L. Maulden-Entergy Endowed Chair and Distinguished Professor of Information Science at University of Arkansas and Director of the Center of Social Media and Online Behavioral Studies. He researches social computing, deviant behavior modeling, group dynamics, social-cyber forensics, data mining, and privacy.

Major Rick Galeano is a US Army officer who has served at NATO's Joint Force Command Brunssum. He lectures at NATO School Oberammergau, the Royal Danish Defence College and the Baltic Defence College.

Dr Rebecca Goolsby developed and heads a NATO Research Technology Group on Information Technologies and Crisis Response, currently focused on projects in Europe. Her research portfolio focuses on information technology and its social and cultural implications for peacebuilding, disaster response, and civil society.

Introduction

The use of social media has exploded in the last few years and continues to grow rapidly. A recent report by Smith et al.[1] shows that there are about 1,3 billion users on Twitter with an average of 100 million active daily users, including 65 million users in the United States alone. In addition to Twitter, Facebook—the largest social media site in the world—has about 1,65 billion users, with about 167 million active daily users in the United States and Canada who spend an average of 20 minutes per day on Facebook.[2] Once primarily used for entertainment and communicating with friends and acquaintances, social media platforms are increasingly used to influence others, spread [mis]information, disseminate propaganda, and invite people to protests and revolutions. Social media has helped facilitate change in many countries. For example, when Mr Mohamed Bouazizi, a 26-year-old Tunisian fruit vendor, set himself on fire on 18 December 2010 in front of a government building, social media helped unify the socio-political unrest and shaped the narrative for the protest movement, which ultimately caused President Zine El Abidine Ben Ali to step down. As reported by the US National Public Radio,[3] that act was captured on camera, disseminated through social media, and broadcast on many national and international TV channels. This encouraged activists in many other countries to protest against their authoritarian regimes in the Middle East and collectively gave rise to what is called the 'Arab Spring'.

[1] Smith, Craig, 'By The Numbers: 170+ Amazing Twitter Statistics', *Digital Marketing Ramblings*, 30 April 2016.

[2] Ibid; Smith, Craig, 'By The Numbers: 200 Surprising Facebook Statistics (April 2016)',*Digital Marketing Ramblings*, 1 June 2016

[3] 'The Arab Spring: A Year Of Revolution', *National Public Radio*, 17 December 2011, All Things Considered.

Several journalistic accounts provide empirical evidence that deviant groups perform strategic and tactical manoeuvres of information using social media to exploit local grievances, steer public opinion, polarise communities, and incite crowd violence. We define a 'deviant group' (DG) as a group of individuals that organises a harmful activity affecting cyberspace, physical space, or both, i.e. the 'cybernetic space'.[4] There are many examples of very well known deviant groups, such as the so-called the Islamic State in Iraq and Syria/Levant, also known as ISIS, ISIL, or Daesh. Also, the cyber criminals or hacker networks that use social media as a platform to coordinate cyber attacks,[5] sell various programs/software that can capture sensitive financial data,[6] or sell those financial data using online forums to make a profit are considered to be deviant groups.[7] Another example of deviant groups can be found in the recent Ukraine-Russia conflict, where sites like VKontakte—a Russian social media platform, LiveJournal, Twitter, YouTube, and other blogging platforms (e.g. Tumblr, etc.) have been used as propaganda machines, justifying the Kremlin's policies and actions.[8] According to *Interpret Magazine*, the Kremlin recruited over 250 'trolls', people hired to disseminate false information, rumours, or propaganda on popular blogs with large audiences, and paid each of them $917 per month to work around the clock producing posts on social and mainstream media. The trolls would create a stream of invective against pro-Ukrainian media and Western news sources writing unflatteringly about Russia, and by posting numerous comments and blog posts each day using multiple 'sock puppet' accounts, clone accounts, and by working in small groups, e.g. triads (a group of three individuals). Such 'troll armies' (or 'web brigades') piggyback on the popularity of social media to disseminate fake pictures and videos, coordinating effective disinformation campaigns to which even legitimate news organisation sometimes fall prey.[9] To stem the tide of fakery, or at least to increase awareness of the problem, online crowdsourcing-based efforts like StopFake.org, the European External Action Service (EEAS), the East Strategic Communication Task Force and its program to fight disinformation (@EUvsDisInfo), and the Estonian organisation PropaStop.Org have been created to identify and debunk fake imagery and stories about the war in Ukraine. However, such efforts are severely limited and easily outnumbered by the troll armies.

[4] Samer Al-khateeb and Nitin 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.

[5] Samer Al-khateeb et al., 'Exploring Deviant Hacker Networks (DHN) On Social Media Platforms', *The Journal of Digital Forensics, Security and Law:* 11, no. 2 (2016): 7–20.

[6] Holt, Thomas J., 'Examining the Forces Shaping Cybercrime Markets Online', *Social Science Computer Review* 31, no. 2 (2013): 165–77.

[7] Holt, Thomas J., 'Exploring the Social Organisation and Structure of Stolen Data Markets', *Global Crime* 14, no. 2–3 (2013): 155–74.

[8] Allen, Michael, 'Kremlin's 'Social Media Takeover': Cold War Tactics Fuel Ukraine Crisis', *Democracy Digest, National Endowment for Democracy*, 10 March 2014; Bohlen, Celestine, 'Cold War Media Tactics Fuel Ukraine Crisis', *The Times*, 10 March 2014

[9] Sindelar, Daisy, 'The Kremlin's Troll Army: Moscow Is Financing Legions of pro-Russia Internet Commenters. But How Much Do They Matter?', *The Atlantic*, 12 August 2014.

With the growth of easy-to-use technology, mobile devices, and the wide availability of programming tools and hacks, the dissemination of propaganda on social media is becoming easier. Research shows that most Internet traffic, especially on social media, is generated by 'botnets',[10] or computer programs coordinated across numerous computers that can be scheduled to perform various tasks on the behalf of the user. In addition to botnets, individuals are hired to troll social media sites, primarily blogs, to help in disseminating propaganda, especially during times of crisis.[11] Throughout this article, we will use the term 'bots' to refer to a collection of bots that are not necessary connected, while we will use the terms 'botnet' and 'automated social actors/agents' (ASAs) to refer to networks of connected and coordinated bots.

The fragmented and diverse nature of Internet discourse and news distribution creates a gap-filled territory for exploitation by social bots and hybrid human/bot collaborations that engage in information conflicts, or 'trolling', and in the dissemination of messages. Nowhere is this more evident than in the strange byroads of Twitter. Social bots carrying *Russian Times* stories and topics have been running rampant in Twitter feeds. So much so that these bots can even be identified in studies that only look at the 1% of the Twitter feeds one can access via Twitter's most widely used APIs, i.e. the REST API. The output generated by these botnets is often strange and it is difficult to see their interference as compelling, or even interesting, but their presence crowds out legitimate voices in the stream, even if bot messages are spouting nonsense. Hordes of bots and hybrid human/bot posts flooded Twitter's algorithms with fabricated and manipulated information. By occupying these channels, bots were able to halt a global outpouring of concern by the people before it gained momentum.

Bot-controlled information dissemination can move a given message into the answer stream suggested for the keywords given by people using Twitter or other search engines. There is a definite art to this process. If done well, such methods can bump a topic up into 'top trends'—showing the world that a topic is popular on the world stage of public interest. Conversely, sending too many messages will trigger Twitter or other search engines' spam prevention algorithms, resulting in detecting the manipulation and suspending the accounts.

Botnet and hybrid human/bot campaigns also have other objectives. They can drive up the Google PageRank scores for articles, expanding the reach of Russian spin on news stories. For example, a Google search on 'MH17 and deception' pulls up, as first and second posts, attacks on the West as having been the perpetrators of deception, rather than the Russians. [Dis]information was widely propagated by the anti-Western websites *21st Century Wire*[12] and *Global Research,*[13] which promoted the

[10] Cheng, Alex and Mark Evans, 'Inside Twitter An In-Depth Look at the 5% of Most Active Users', (Sysomos Inc., 2009).

[11] Sindelar, 'The Kremlin's Troll Army'.

[12] Helton, Shawn, 'Flight MH17 Conjures MH370, Exposing Western Deception, Leading To More Questions', *21st Century Wire*, 19 July 2014.

[13] Helton, Shawn, 'Flight MH17 Conjures MH370, Exposing Western Deception, Was It a Staged Event?', Blog, *Global Research,* 19 July 2014.

story that the downing of Malaysian Airlines flight MH17 over Ukraine was a staged event and alleged widespread Western manipulation of media; these sites achieved page ranks over and above the popular mainstream article from *The Economist.*[14] *The Economist* has a print circulation of over 1m and monthly page views over 34m.[15] This indicates that manipulation of PageRank scores is possible, although the influence of other conspiracy sites, forums, mailing lists, and the like should not be discounted as 'push factors' in building PageRank scores. Wild, tantalising rumours can energise global social networks of conspiracy theorists, throwing gasoline on the fire of speculation among rabid anti-Western ideologues. Certainly, this firestorm was kindled and initiated from the postings and reportage of *RT* and *PressTV*, as well as other Russian-owned news organisations. *The Guardian,*[16] the *BBC,*[17] and the *Washington Post*[18] catalogued that conspiracy theorists around the world had a field day with the MH17 tragedy.

Social media has undoubtedly helped facilitate change.[19] There are several examples, where social media has helped transform the socio-political landscape of a country or an entire region (e.g. Arab Spring),[20] helped coordinate humanitarian assistance and disaster relief operations (e.g. the humanitarian crisis during the Nepal earthquake),[21] and shaped people's decisions, plans, behaviours, or beliefs (e.g. during the spread of an infectious disease).[22] The powerful ability of social media platforms to connect with the masses and influence their behaviour has attracted many groups and organisations.[23] In some cases, groups or organisations harness the power of social media to provoke hysteria and influence public opinion to encourage the destabilisation of a region through the dissemination of propaganda about global or local events.[24]

The deviant practices conducted over modern information and communication technologies (ICTs), especially social media, call for an in-depth study to better understand the new strategic communication and its evolution over time.

[14] 'Russia, MH17 and the West A Web of Lies', Blog, *The Economist*, 26 July 2014.

[15] Moore, Sue, 'The Economist - Worldwide Brand Report', *The Economist*, 8 November 2016.

[16] Reidy, Padraig, 'MH17: Five of the Most Bizarre Conspiracy Theories', *The Guardian*, 22 July 2014.

[17] De Castella, Tom, 'Malaysia Airlines MH370: The Persistence of Conspiracy Theories', *BBC News*, 8 September 2014.

[18] Dewey, Caitlin, 'A Comprehensive Guide to the Web's Many MH17 Conspiracy Theories', *The Washington Post*, 18 July 2014.

[19] Lutz, Catherine, 'Is Social Media a Dangerous Force Against Democracy?', *The Aspen Idea Blog,* 6 August 2014; Shirky, Clay, 'The Political Power of Social Media: Technology, the Public Sphere, and Political Change', *Council on Foreign Relations* 90, no. 1 (February 2011): 28–41; Brooking, T. Emerson and P.W Singer, 'War Goes Viral: How Social Media Is Being Weaponized across the World', *The Atlantic*, November 2016.

[20] Howard, Philip N. et al., 'Opening Closed Regimes: What Was the Role of Social Media during the Arab Spring?', *Social Science Research Networks*, 17 April 2015.

[21] Preiss, Danielle, 'How Social Media Is Helping Nepal Rebuild after Two Big Earthquakes', *Quartz India,* 19 May 2015.

[22] Schmidt, Charles W., 'Trending Now: Using Social Media to Predict and Track Disease Outbreaks', *Environmental Health Perspectives* 120, no. 1 (2012): 30–33.

[23] Tatham, S. A., *Strategic Communication: A Primer*, (Shrivenham: Defence Academy of the United Kingdom, Advanced Research and Assessment Group, 2008).

[24] Lutz, 'Is Social Media a Dangerous Force?'; Tatham, *Strategic Communication: A Primer.*

This study aims to provide a systematic analysis of botnets, their evolution, and their exploitation for disseminating propaganda through social media. We anticipate that this study will help authorities assess the state of propaganda dissemination and disinformation campaigns conducted on social media, develop strategies to counter such strategic communications, and enhance overall cyber operations.

In this study, we focus on two events, the 2014 Crimean Water Crisis[25] and the 2015 Dragoon Ride exercise[26] to investigate such strategic communications, especially the role of botnets in propaganda dissemination campaigns. We collected data from social media, including blogs and Twitter, during the two events mentioned above. Using socio-computational methodologies, we are able to identify the 'seeders of information' (nodes that work as sources of information, i.e. a node that supplies content to the bot) to the botnets, and the communication and coordination strategies used in each event. A striking observation was made in the case studies, i.e. **the botnets deployed for propaganda dissemination have evolved tremendously by becoming increasingly deceptive and well coordinated.** More specifically, we sought answers to the following research questions:

- Who is responsible for propaganda dissemination in the 2014 Crimean Water Crisis and 2015 Dragoon Ride exercise events?
- What role do botnets play in propaganda dissemination campaigns for these events?
- What strategies are used in each case?
- How did botnets evolve over 2014–2015? And what can be learned from their evolution trajectory?
- Is there an organisational structure among bots, i.e. who is responsible for seeding the information (or rather, misinformation) to these bots? Are these bots working in collusion? Are there other more sophisticated roles played by specific bots to effectively and efficiently coordinate propaganda campaigns in social media? For example, do bots act as brokers to bridge different bot network groups? Can we identify such roles and/or positions?
- What are other structural communication and/or coordination patterns characteristic to botnet propaganda dissemination networks?
- Can we develop predictive models and tools that are able to detect botnet behaviours?

[25] 'Russia Fears Crimea Water Shortage as Supply Drops', *BBC News*, 25 April 2014.

[26] Defense Media Activity DoD News, 'Operation Atlantic Resolve Exercises Begin in Eastern Europe', 24 March 2015.

We are making the following contributions toward answering these questions:

- We study a phenomenon commonly used to disseminate propaganda on social media.
- We propose step-by-step methodologies that can be used to analyse propaganda dissemination.
- We document coordination strategies among bots that enhance the reachability of their propaganda messages.
- We have identified an organisational structure among bots, where a real-person feeds misinformation to a network of bots. Further, a number of bots are programmed to act as brokers, feeding this information to bots in other network groups.
- We identify sophisticated coordination structures among bots corresponding to collective behaviours to disseminate propaganda.
- The findings will inform the development of predictive models and eventually result in tools that can assist in the detection of bots.

The rest of the article is organised as follows. The next section reviews the literature summarising key research studies conducted in the domain of identifying bots in social media. The third section provides a brief description of the data that was collected for the two events, the 2014 Crimean Water Crisis and the 2015 Dragoon Ride exercise, the methodologies that were used to study the botnets, our analysis, and our findings. We outline our conclusions with implications of the research in the fourth section. And in the final section, we shed light on this evolving research area, especially propaganda analysis in the modern ICT and social information system space, and envision the next phase of work.

Literature Review

Bots are not a new phenomenon. They have been studied previously in literature in a variety of domains, such as Internet Relay Chat,[27] online gaming e.g. World of Warcraft (WoW),[28] and more recently behavioural steering through misinformation dissemination on social media.[29]

[27] Anestis, Karasaridis, Brian Rexroad, and David Hoeflin, 'Wide-Scale Botnet Detection and Characterization', in Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets, vol. 7 (Cambridge, MA, 2007); Rodríguez-Gómez, Rafael A., Gabriel Maciá-Fernández, and Pedro García-Teodoro, 'Survey and Taxonomy of Botnet Research through Life-Cycle', *ACM Computing Surveys (CSUR)* 45, no. 4 (2013): 45.

[28] Ackerman, Mark S., Jack Muramatsu, and David W. McDonald, 'Social Regulation in an Online Game: Uncovering the Problematics of Code', in Proceedings of the 16th ACM International Conference on Supporting Group Work (ACM, 2010), 173–182; Karasaridis, Rexroad, and Hoeflin, 'Wide-Scale Botnet Detection and Characterization'.

[29] Protalinski, Emil, 'Facebook: 5-6% of Accounts Are Fake, *ZDNet*, 8 March 2012; Hegelich, Simon and Dietmar Janetzko, 'Are Social Bots on Twitter Political Actors? Empirical Evidence from a Ukrainian Social Botnet', in Tenth International AAAI Conference on Web and Social Media (International AAAI Conference on Web and Social Media (ICWSM-16), Cologne, Germany: AAAI, 2016), 579–82.

One of the earliest bots emerged in 1993 in an Internet Relay Chat (IRC)—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.[30] Shortly thereafter, the use of bots in IRC became very popular due to the simplicity of implementation and their ability to scale IRCs.[31] The bots evolved over time (gained functionality), and the tasks these bots were assigned became more complicated and sophisticated.[32] Botnets were used in the Multi-User-Domains (MUDs) and Massive Multiplayer Online Games (MMOGs). The emergence of Multi User Domains emphasised the need for Automated Social Actors (ASAs) to enhance the playing experience. As the online gaming market grew, the need for more advanced bots increased. In MMOGs, such as the World of Warcraft (WoW) unauthorised game bots emerged. These unauthorised bots enhance and trigger mechanisms for the players, often by sitting between the players' client application and the game server. Some of these bots were also able to play the game autonomously in the absence of the real player. In addition, some bots were also able to damage the game ecologies, i.e. amass experience points or game currency (virtual gold, etc.).[33]

Social media has emerged over the last fifteen years, and the use of bots in this context has only recently been observed. In a study conducted by Facebook in 2012, 5–6% of all Facebook user accounts are fake accounts. This means that there are about 50 million user accounts on Facebook that do not belong to real people.[34] Some of these bots are very sophisticated and some even try to mimic human behaviour, which makes discovering, detecting, or capturing them a challenging task.[35]

Abokhodair et al. studied the use of social botnets regarding the conflict in Syria in 2012.[36] The Abokhodair et al. study focused on one botnet that lived for six months before Twitter detected and suspended it.[37] The study analysed the life and the activities of that 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, mobilisation of resistance/support, mobilisation 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 a bot tweeting in Arabic or English differed from a non-bot or legitimate user tweeting in Arabic or English. For example, bots tend to share more news articles, fewer opinion tweets, no testimonial tweets, and fewer conversational

[30] Rodríguez-Gómez, Maciá-Fernández, and García-Teodoro, 'Survey and Taxonomy of Botnet Research'.

[31] Karasaridis, Rexroad, and Hoeflin, 'Wide-Scale Botnet Detection and Characterization'.

[32] Abokhodair, Norah, Daisy Yoo, and David 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 (ACM, 2015), 839–851.

[33] Ibid.

[34] Protalinski, 'Facebook: 5-6% of Accounts Are Fake'.

[35] Yazan Boshmaf et al., 'Key Challenges in Defending against Malicious Socialbots', in Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats (USENIX Association, 2012), 12–12.

[36] Abokhodair, Yoo, and McDonald, 'Dissecting a Social Botnet'.

[37] Ibid.

tweets than any legitimate Arabic or English Twitter user. They also classified bots based on the content they posted, the length of time before the bot was suspended, and the type of activity the bot engaged in (tweet or retweet) into the following categories:

- **Core Bots:** have three sub-categories:
    1. **Generator Bots:** tweet often, but seldom retweet anything.
    2. **Short-Lived Bots** tweet seldom, but retweet often and last for fewer than six weeks before Twitter suspends the account.
    3. **Long-Lived Bots** tweet seldom, but retweet often and last for more than 25 weeks before Twitter suspends the account.
- **Peripheral Bots:** are Twitter accounts lured into participation in the dissemination process. Their task is to retweet one or more tweets generated by the core bots.

The difference between their study and ours is that we are focusing on the evolution and sophistication of botnets exploited for conducting propaganda campaigns. Further, we show methodologies that help detect such behaviours and try to understand the roles and positions assumed by the bots within their group (such as brokers who serve as bridges between different parts of the network or sub-networks) for affecting various information manoeuvres.

In the article, entitled 'The Rise of Social Bots',[38] Emilio et al. did a literature review of more than 43 articles that mainly discussed bot detection methods. The authors talked about the effects of bots on society and the economy, and how bots can amplify the visibility of misinformation. The authors also categorised bot identification approaches into three classes:

- Detection systems based on 'social network information'
- Detection systems based on 'crowdsourcing and leveraging human intelligence'
- Detection systems based on 'machine learning methods'

The authors discuss pros and cons for each method. Then they conclude with a call to understand bot coordination strategies and identify the 'puppet masters' (what we call the 'seeders of information') as bots are continuously changing and evolving. They also mention the need to develop tools that combine the three categories for better bot detection. Our work here addresses the needs identified by the research community. We are studying and documenting bot behaviour and the strategies bots use to disseminate propaganda, which will enhance existing models analysing information actors and their behaviours in social media spaces.

[38] Emilio Ferrara et al., 'The Rise of Social Bots', *Communications of the ACM 59*, no. 7 (24 June 2016): 96–104.

ISIL is another example of a deviant group using botnets on social media to disseminate propaganda. They used botnets to disseminate videos of their beheadings to the hostages they captured (e.g. the beheading of Egyptian Copts on 15 February 2015 in Libya,[39] the beheading of the Arab-Israeli 'spy' in on 10 March 2015 Syria,[40] and the beheading of an Ethiopian Christian on 19 April 2015 in Libya).[41] In that work, we studied the 'bipartite network'[42] of ISIL's communication network (i.e. tweets, retweets, and mentions network) to understand how ISIL propaganda videos and images of the beheading of hostages in orange jumpsuits swept across social media at the time of each event. We collected data for the aforementioned events and found out that the majority of the data consisted of retweets, indicating that Core Bots, both Short-Lived and Long-Lived, and Peripheral Bots were very active in retweeting the messages posted by ISIL accounts. We also found out that the tweets contained an unusually high number of URLs in their content, and many of them contained characters that would not be published by real-humans, i.e. rubbish or code characters. In addition, we found that the accounts posted many tweets in a short period of time and the account names differed only by a single character, such as a number added to the end or beginning of the account name, etc.[43]

The Evolution of Botnets

In this section, we consider the 2014 Crimean Water Crisis and the 2015 Dragoon Ride Exercise as case studies for our investigation into the role bots play in propaganda dissemination and the evolution of bot behaviour. The details of each case study, along with a description of the data, the methodology, and our findings are presented here.

Case Study 1: The 2014 Crimean Water Crises

The Nature of the Propaganda

Russia's annexation of the Crimean peninsula on 16 March 2014 met with international discontent. Both the United Nations and the NATO Secretary General have condemned this expansion of the Russian sphere of influence. Civil unrest and political instabilities in both Russian-annexed Crimea and in Ukraine resulted in significant humanitarian crises due to economic impacts, changes in civil authority, and deep uncertainties about shifting political and economic relationships. Grievances, requests for help, and on-the-ground reports on the developing conflict

[39] CNN Staff, 'ISIS Video Appears to Show Beheadings of Egyptian Coptic Christians in Libya', *CNN*, 16 February 2015.

[40] 'ISIL Executes an Israeli Arab after Accusing Him of Been an Israeli Spy', *TV7 Israel News*, 11 March 2015.

[41] Shaheen, Kareem, 'Isis Video Purports to Show Massacre of Two Groups of Ethiopian Christians', *The Guardian*, 19 April 2015; Al-khateebm Samer and Nitin Agarwal, 'Examining Botnet Behaviors for Propaganda Dissemination: A Case Study of ISIL's Beheading Videos-Based Propaganda', (Data Mining Workshop (ICDMW), 2015 IEEE International Conference on, IEEE, 2015), 51–57.

[42] Bipartite network - a network containing two types of nodes that are connected through edges/relationships, i.e. a network of Twitter User-Text and a network of Twitter User-URL is considered a bipartite network because the Twitter user is one type of node and the URLs or Text itself is another type of node

[43] Ibid.

were reported on a variety of open source platforms including blogs, news websites, Twitter, Facebook, and other open source channels such as YouTube.

The economic impact of the annexation dominated online media coverage. Several stories published by Russian news agencies, including *ITAR-TASS*, claimed that Ukraine's government had ceased work on the North Crimean Canal that carries water from the Dnepr to Crimea.[44] *RT* reported that satellite images showed Ukraine deliberately trying to cut off the Crimean peninsula's water supply by building a dam, while Russian scientists were trying to find ways to supply Crimea with fresh water in the meantime.[45] A *New York Times* article reported that quality of life was deteriorating in Russian-annexed Crimea—a water shortage was observed, Crimean farms were drying, food supplies were inadequate, and price of basic goods, such as milk and gas, had doubled.[46] The article further stated that the tourism economy was also suffering and was down by one third from the previous year; few banks were operating—Ukrainian banks had closed, Russian banks were barely open, and Western banks feared sanctions for continuing to operate in Crimea; only Russian channels were providing television and cable services; and telecommunications were erratic as carriers shifted from Ukrainian to Russian providers. The Russian media largely blamed Ukraine government officials for these problems. Several social media outlets, including blogs, picked up the pro-Russian narrative and amplified it further suggesting that Ukraine was colluding with the West in direct conflict with Russia against the will of Crimean citizens.[47] The propaganda from pro-Russian mainstream media and social media sources was further intensified by bots on Twitter. Botnets effectively disseminated thousands of messages in relation to the Crimean water crisis. These bots were disseminating anti-West and pro-Russia news articles in a bid to provoke hysteria. Numerous bots were simply tweeting the same article after copying it to various websites and blogs, making it appear as if the article were independently posted on different URLs. In other words, bots were cloning the [mis]information, creating an echo chamber, and misleading the public.

Data Description

We used an integrated data collection strategy from disparate publicly available online sources that were identified as relevant for the crises. Often content (reports, images, videos, articles, etc.) originated on one social media site and was diffused to many other sites without attribution. It was therefore imperative to track multiple social media sites to identify implicit interconnections. Using hyperlinks, a snowball data collection approach was used. We used the following keywords 'Ukraine', 'Ukraine Crisis', 'Euromaidan', 'Automaidan', and 'Ukraine's Automaidan Protestors' to collect data about the crisis. Initially the dictionary of keywords for crises/events are manually seeded, but evolve automatically. We identified the popular blog posts for the Ukraine-Russia conflict and, by cross-referencing with Twitter data, we found

[44] Pavlishak, Alexel, 'Water Supply Problem in Crimea to Cost $247- 417 Million - Kremlin Aide', *TASS Russian News Agency*, 28 April 2014.

[45] 'Ukraine Builds Dam Cutting off Crimea Water Supply', *RT Question More*, 10 May 2014.

[46] Macfarguhar, Neil, 'Aid Elusive, Crimea Farms Face Hurdles', *The New York Times,* 7 July 2014.

[47] Jerome, Sara, 'Ukraine-Russia Conflict Results In 'Water War'', *Water Online*, 4 August 2014.

which posts were diffused most often on Twitter. We used the tools TweetTracker,[48] and NodeXL[49] to collect Twitter data for the period between 29 April 2014 8:40:32 PM and 21 July 2014 10:40:06 PM UTC. This resulted in 1,361 unique tweets, 588 unique Twitter users, and 118,601 relations between the Twitter users. There are four basic types of relations in the Twitter data: *follows*, *mentions*, *replies*, and *tweets*.

Methodology to Identify Botnets

During the research period (April 2014–July 2014) Ukrainian, Russian, and global attention shifted away from Crimea to the active conflict in Southeast Ukraine. Local or regional information can often be found by searching under hashtags in the local language, rather than in English. #crimea, in both Russian and Ukrainian forms, had erratic results from day to day using the same filtering algorithm, as topics such as the end of the ceasefire and the advance of troops into Southeast Ukraine began to take precedence.

There are 'natural social rules and principles' on Twitter that people adhere to in order to increase their followers, e.g. making the choice to follow everyone who follows a user, or by asking those you follow to follow you back in reciprocity. In the last several years, a new artificial means of amplifying followerships has emerged in the form of 'social bots'—scripted codes that mimic human users and serve as super-spreaders of information, opinion, malware, self-promotion, promotion of news stories, or advertisement through fake Twitter accounts. Social bots that serve no purpose other than to move specially-crafted messages through the Twitter environment. These artificial methods can be used to promote particular points of view/purported facts, and can serve as a means to amplify these points of view in the promotion of blogs and other content, far beyond the reach that the quality or representativeness of said viewpoint would achieve by non-artificial means.

By analysing the tweets and their content we observed the following anomalous behaviours:

1. Many tweets were identical, i.e. different Twitter users posted same tweets. Note that identical tweets are not the same thing as retweets.
2. The frequency of the tweets was unusually high, i.e. a large number of tweets were posted within a very short space of time—a behaviour that is humanly impossible.
3. All tweets contained 'short' links, pointing to the same article on a specific website.
4. All of the tweets were bracketed within a pair of hashtags, i.e. there is a hashtag at the beginning and end of every tweet.

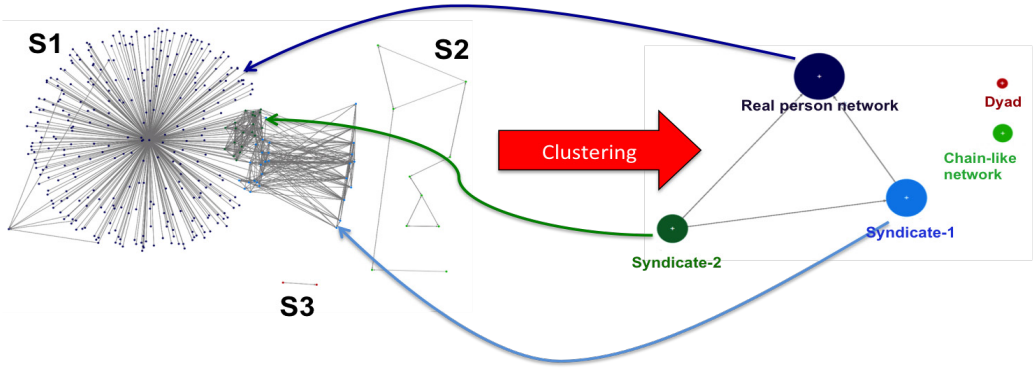
[48] Kumar, Shamanth et al., 'TweetTracker: An Analysis Tool for Humanitarian and Disaster Relief', in ICWSM, 2011.

[49] Smith, Marc A. et al., 'Analyzing (Social Media) Networks with NodeXL', in Proceedings of the Fourth International Conference on Communities and Technologies (ACM, 2009), 255–264.

5. These hashtags are not related to the content of the tweet. This indicates the presence of 'misdirection' and 'smoke screening' strategies.[50] More specifically, the hashtags correspond to the names of cities, states, and countries around world, completely unrelated to the content of the tweet or to the linked website. A possible explanation for using such a behaviour, also known as 'hashtag latching', could be to achieve greater exposure for the messages.
6. Precise repetitive patterns and correlations were observed, e.g. users with Arabic names did not provide location information, while users with non-Arabic names provided locations in the Arab/Middle-East regions.

Such anomalous behaviour is characteristic of a computer software program, or of a bot that can operate on Twitter autonomously.

Figure 1. Three sub-networks with unusual structural characteristics in S1 are observed, then the Girvan-Newman clustering algorithm is applied to the network. On the left are the expanded clusters and on the right is the collapsed view of the clusters. Five clusters are identified.



By analysing the friends/followers network (social network) of the accounts related to the data we collected, we found that it had three sub-networks: S1, S2, and S3 (see Figure 1). The sub-network S1 exhibited unusual structural characteristics. The other two sub-networks, the 'chain-like' S2 and 'dyadic' S3 sub-networks, were ignored due to their relatively small size and lack of anomalous behaviours. We applied the Girvan-Newman clustering algorithm[51]—an algorithm that detects communities in a network based on how closely the nodes are connected—to the S1 network and found that the network had five clusters (communities or groups of nodes), as shown in Figure 1. Our analysis showed that S1 had one star-shaped and two clique-style groups of nodes. The centre of the star-shaped network belonged to a 'real-person'[52] node, or Twitter account, which was connected to 345 bots out of 588 twitter handles in this network (see Figure 2). This real-person is the owner/operator of the specific webpage that all the other bots were referring to with different shortened links.

[50] Abokhodair, Yoo, and McDonald, 'Dissecting a Social Botnet'; Ferrara et al., 'The Rise of Social Bots'.

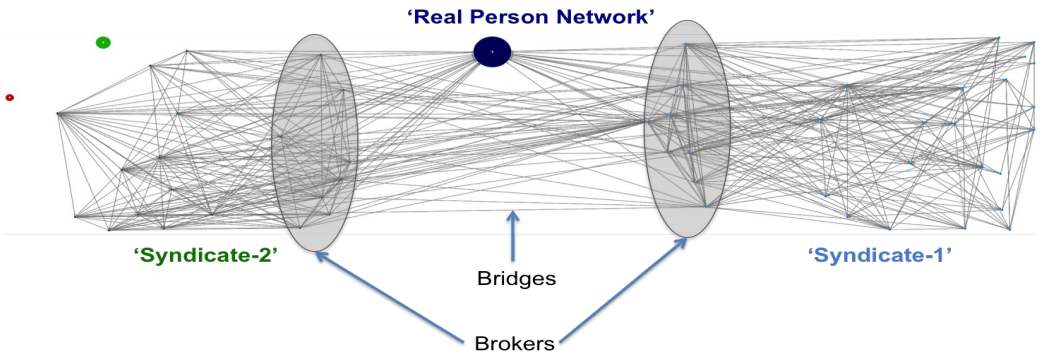
[51] M. Girvan and M. E. J. Newman, 'Community Structure in Social and Biological Networks', Proceedings of the National Academy of Science of the United States of America 99, no. 12 (6 April 2002): 7821–26.

[52] The term 'real-person' is used so as not to disclose the identity of this node.

Un-collapsing the 'real-person' network revealed its star-shaped structure, where 'real-person' is the central node. It also shows the connections to the other two-syndicate groups, viz. syndicate-1 and syndicate-2. Close examination of these ties revealed that the members of the syndicate followed the 'real-person' node, and not the other way. **We thus concluded that 'real-person' is the most central node of this entire bot network and the one feeding information to the bots.**

While un-collapsing the syndicate-1 and syndicate-2 networks revealed dense connections among their members and inter-group connections with the other groups, the 'real person' network and 'syndicate-2', closer examination of the intra-group ties revealed mutually reciprocated relationships, suggesting use of **the principles '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.[53]

Figure 2. The real person network is connected to broker bots that coordinate the dissemination of propaganda through the bots in their respective syndicates.



Unlike the 'real person' network, there is no single most central node in these networks, indicating an absence of a hierarchical organisation structure in the 'syndicate-1' and 'syndicate-2' networks. Further analysis showed that the broker nodes act as interfaces between the group members and other groups. The broker nodes of the two syndicates established bridges that facilitated tweet diffusion across the syndicates. The broker nodes were primarily responsible in connecting with the 'real person' network, specifically the 'real person' node, which is also the most influential node. This indicates that **the bot network was using a sophisticated coordination strategy,** as can be seen in Figure 2.

[53] Ghosh, Saptarshi et al., 'Understanding and Combating Link Farming in the Twitter Social Network', in Proceedings of the 21st International Conference on World Wide Web (ACM, 2012), 61–70; Labatut, Vincent, Nicolas Dugue, and Anthony Perez, 'Identifying the Community Roles of Social Capitalists in the Twitter Network' (IEEE/ACM International Conference on Advances in Social Network Analysis and Mining (ASONAM), China, 2014), 8.

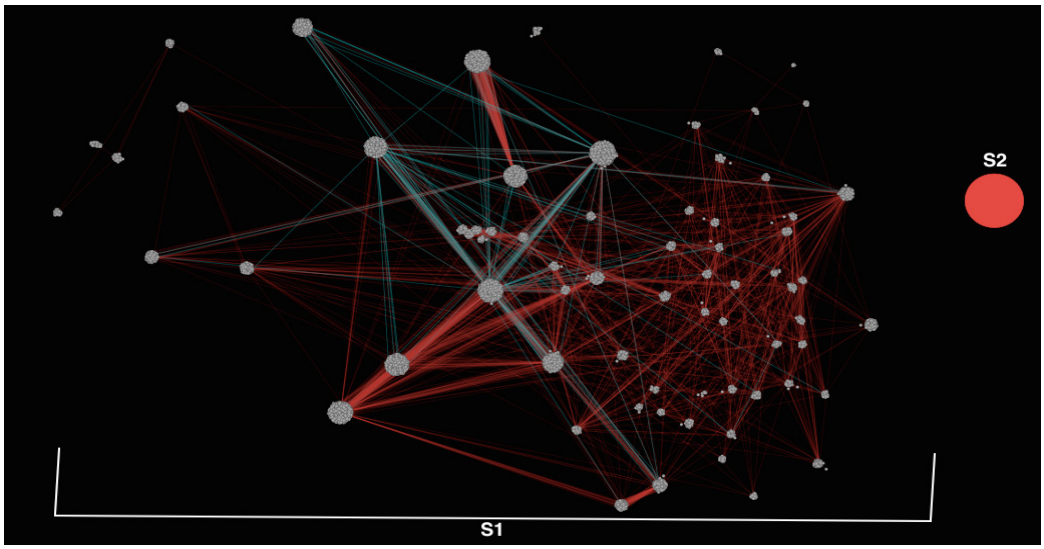
Case Study 2: The 2015 Dragoon Ride Exercise

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. The US troops, nicknamed 'Dragoons', were sent on a transfer mission crossing five international borders and covering more than 1,100 miles to exercise the unit's maintenance and leadership capabilities, and to demonstrate the freedom of movement that exists within NATO.[54]

Many opponent groups launched campaigns to protest the exercise, e.g. 'Tanks? No Thanks!',[55] which appeared on Facebook and other social media sites, promising large and numerous demonstrations against the US convoy.[56] Czech President Miloš 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.[57] The *RT* website also reported that the Czechs were not happy with the procession of the 'U.S. Army hardware'.[58] 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.

Figure 3: Two sub-networks, S1 and S2. S1 is un-collapsed while S2 is collapsed. Edges in red denote mutually reciprocal relations (bidirectional edges) while edges in blue colour denote non-reciprocal relations (unidirectional edges).



[54] DoD News, 'Operation Atlantic Resolve Exercises Begin in Eastern Europe'.

[55] "Tanks? No Thanks!': Czechs Unhappy about US Military Convoy Crossing Country', *RT Question More,* 22 March 2015.

[56] Sindelar, Daisy, 'U.S. Convoy: In Czech Republic, Real-Life Supporters Outnumber Virtual Opponents', *Radio Free Europe/Radio Liberty*, 30 March 2015.

[57] 'Czechs Plan Multiple Protests Of US Army's Operation Dragoon Ride', *Sputnik News*, 2 March 2015.

[58] 'Tanks? No Thanks!', *RT*.

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, an online social media analysis tool available at www.scraawl.com. We collected data on this network of bots and studied its structure in an attempt to understand how they operated and to compare them to the Crimean water crisis bots. Here we provide a description of the dataset and our findings.

Data Description

We collected data for the period between 8 May 2015 8:09:02 PM and 3 June 2015 11:27:31 PM UTC of 90 Twitter accounts that were identified 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 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 (a tool for social media data collection and analysis) that included friend-follower relations and tweet-mention-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.

Data Analysis & Findings

We analysed the friend/follower networks (social network) of the bot accounts. We applied the Girvan-Newman clustering algorithm[59] to this network and found that the network had two clusters, S1 and S2, as shown in Figure 3. 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.

Closer examination of the S1 cluster revealed that the members of that network were more akin to the syndicate network of the Crimean Water Wrisis botnets. Further examination of the within-group ties, revealed a mutually reciprocated relationship (the nodes followed each other), suggesting that the principles of FMIFY and IFYFM were in practice—a behaviour that was also observed among the Crimean Water Crisis botnet.

Unlike the previous case, this network had no central node (i.e. there was no single node feeding information to the other bots, or seeder of information). This indicated the absence of a hierarchical organisational 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

[59] Girvan and Newman, 'Community Structure in Social and Biological Networks'.

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.[60]

Focal Structure is an algorithm that was implemented by Sen et al.[61] to discover an influential group of individuals in a large network. 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.[62] 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.[63] 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[64] 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.[65]

FSA has been tested on many real world cases such as the Saudi Arabian Women's Right to Drive campaign on Twitter [66] 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.

[60] Sen, Fatih et al., 'Focal Structure Analysis in Large Biological Networks', in IPCBEE, vol. 70, 1 (2014 3rd International Conference on Environment Energy and Biotechnology, Singapore: IACSIT Press, 2014). doi:10.7763; Sen, Fatih et al., 'Focal Structures Analysis: Identifying Influential Sets of Individuals in a Social Network', *Social Networks Analysis and Mining* 6 (2016): 1–22.

[61] Sen et al., 'Focal Structure Analysis in Large Biological Networks'; Sen et al., 'Focal Structures Analysis: Identifying Influential Sets of Individuals in a Social Network'.

[62] Girvan and Newman, 'Community Structure in Social and Biological Networks'.

[63] Blondel, Vincent D. et al., 'Fast Unfolding of Communities in Large Networks', Journal of Statistical Mechanics: Theory and Experiment 2008, no. 10 (2008): P10008.

[64] Sen et al., 'Focal Structures Analysis: Identifying Influential Sets of Individuals in a Social Network'; Jaccard, Paul, 'The Distribution of the Flora in the Alpine Zone', *New Phytologist 11*, no. 2 (1912): 37–50.

[65] Sen et al., 'Focal Structures Analysis: Identifying Influential Sets of Individuals in a Social Network'.

[66] Serpil Yuce et al., 'Studying the Evolution of Online Collective Action: Saudi Arabian Women's 'Oct26Driving' Twitter Campaign', in Social Computing, Behavioral-Cultural Modeling and Prediction (Springer, 2014), 413–20.

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.[67]

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[68]—a 35-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 resources, 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 seconds at a time.[69]

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 Figure 4]. 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 Figure 5]. 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.

Although botnets were used to disseminate propaganda during the events of both case studies, 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

[67] Sen et al., 'Focal Structures Analysis: Identifying Influential Sets of Individuals in a Social Network'.

[68] Graham Phillips is a British national contracted as a stringer by the Russian Times (RT). He has produced numerous videos, blogs, and stories in/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. 25 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 3 years.

[69] Seddon, Max, 'How A British Blogger Became An Unlikely Star Of The Ukraine Conflict — And Russia Today', *BuzzFeed News*, 20 May 2014.

more sophisticated approach to identify the organisers 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 behaviour to develop sophisticated approaches/techniques or tools that can deal with predictive modelling of botnets.

Figure 4. 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 red 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 red.

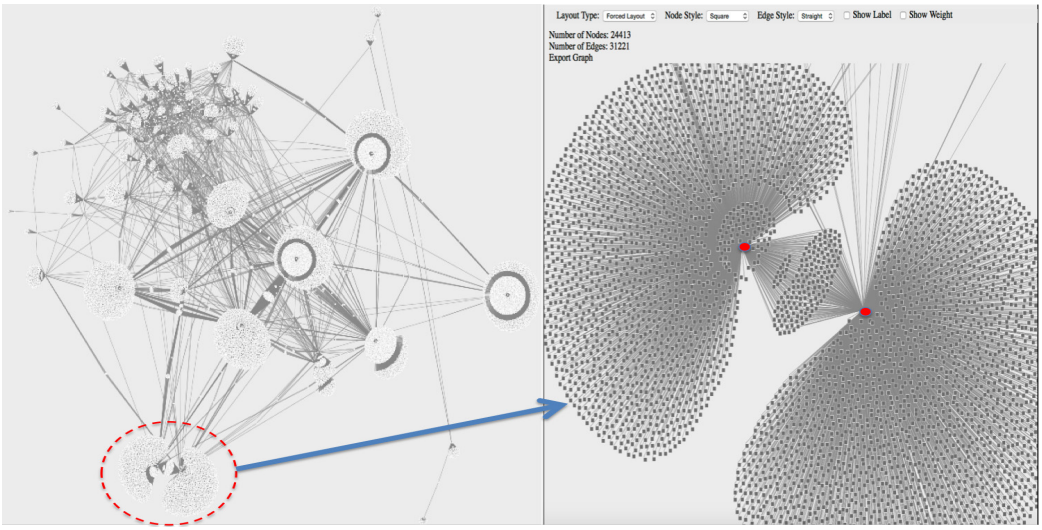
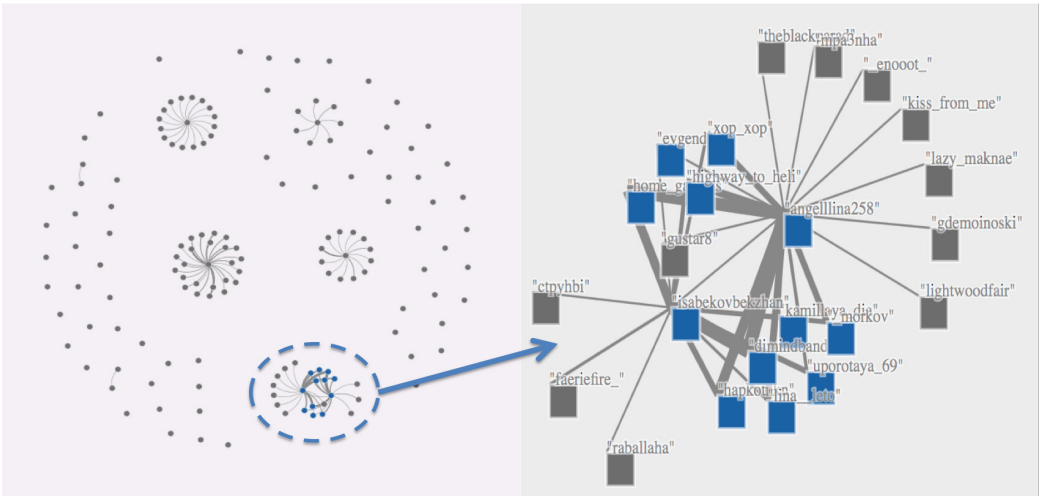


Figure 5. Communication network (tweets, mentions, and replies network) of the botnets. Ten nodes were communicating the most with the two most influential bots in the network.



Conclusion

In conclusion, the affordability and easy-to-use nature of social media has made it a popular choice for communication and seeking information among many people around the world. Social media use has been shifting from entertainment to public discourse, thereby making it a preferred tool for influencing group opinions or achieving political goals by disseminating propaganda or misinformation about various events. This study has observed and analysed the behaviour of botnets during two events, i.e. the 2014 Crimean Water Crises and the 2015 Dragoon Ride exercise. During these two events botnets were used to disseminate pro-Russian, anti-Western, and anti-NATO propaganda. The study shows the complexity of the bot networks that are deployed to disseminate propaganda. The 2014 Crimean Water Crises case study shows an example of an easy-to-capture botnet, while the 2015 Dragoon Ride exercise case study shows a more complex bot network, where sophisticated methods were required to identify dissemination behaviour. In the former case, the seeders of information to the bots were easily identified along with the organisational structure of the bot network, such as the brokers, central bots, communication strategy, etc. Conversely, in the latter case, the seeders of information to the bots were not easily identified. Instead a small number of bots were coordinated to seed the information; individually they were not very influential but collectively they profoundly impacted the dissemination of propaganda. Furthermore, both social networks and communication networks of the bots were examined to identify the organisational structure of the propaganda dissemination process. Sophisticated approaches to network analysis, such as the focal structure analysis approach, were used in the latter case. These findings are strongly indicative of the evolution of botnets deployed for propaganda dissemination. This suggests a need for more intelligent bot detection techniques—techniques that can evolve together with the bot behaviours. The development of such techniques is in line with the need identified by the research community.

Further Discussion and Future Work

In this section we shed light on the evolving research area of propaganda analysis in modern ICTs and the social information system space, envisioning future tasks. We add our voices to the research community calling for developing bot detection tools that can evolve as bot behaviours evolve and change. The cases mentioned in this article, and numerous others, demonstrate strategic and tactical information manoeuvres by adversarial information actors. We are working on a three-step action plan to rigorously study, document, and model such manoeuvres. First, we will systematically categorise bots, based on the published research and on our own empirical observations of the role of information actors (e.g. botnets, trolls) in Russian strategic communications. Second, we will identify and document the various strategies exhibited by independant information actors and coordinated information actors. This will help to enhance state-of-the-art analysis models for information actors and their behaviours in social media spaces. And third, we have observed that many bots disseminate links to blog sites where an individual or a group frames the narrative for disseminating propaganda around various issues. A likely reason

for using blogs to frame narratives is the freedom they afford for writing as much as an author wants and for embedding multimedia (e.g. images, audio bytes, videos) and links to other social media objects, such as tweets, etc. By presenting half-truths, contorted facts, manipulated images, and videos in a cogent manner substantiated by links to other propaganda riddled websites, it is not very challenging to mislead the average reader. To do so effectively one does not need much more than 140 characters. This is where blogs are most helpful—i.e. to develop a story. Bots are used to steer attention to these blogs. The goal of the bots is to bring the propaganda-riddled content to as many eyeballs as possible by employing crafty strategies. We plan to conduct an in-depth analysis of this orchestrated use of social media in propaganda campaigns. More specifically:

A. We plan to conduct cyber forensic analysis by using cyber forensic techniques to find blogs sites or other groups connected to our 'seed' of blogs (the initial set of the URLs we will extract). 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' [70]. One technique that can be used is to find blogs owned by a single owner or managed by the same unique identifier or 'UA' number, e.g. Google Analytics ID. Google Analytics ID is an online analytics tool that allows a website owner to gather some statistics about their website visitors such as their browser, operating system, and country they are from, along with other metadata. ID numbers are embedded in the website HTML code for each user. Such information and other metadata can be obtained from many cyber forensics tools, e.g. Maltego,[71] which is an open source cyber forensics application. This tool and technique was cited in the book title *Open Source Intelligence Techniques* by Michael Bazzell, an FBI cyber crime expert[72] and also reported by *Wired* in 2011.[73] This part of a blog's identification and blog's data collection/crawling will be leveraged in part (b) where we will use and analyse this data.

B. We plan to crawl the data of the blog sites that has propaganda against some of the events and store it in the database of our developed Blogtrackers[74] tool (available at: www.blogtrackers.host.ualr.edu). Blogtrackers is a tool that has the ability to analyse blog data. Blogtrackers has many analysis capabilities, e.g. to identify blog activity patterns, keywords patterns/trends, the influence a blog or a blogger has on a given online community, and to analyse sentiment diffusion in such communities.

[70] Digambar Povar and V.K. Bhadran, 'Forensic Data Carving', in *Digital Forensics and Cyber Crime*, vol. 53, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (Springer Berlin Heidelberg, 2011), 137–48.

[71] 'Maltego', Paterva, *A New Train of Thought*.

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

[73] Alexander, Lawrence, 'Open-Source Information Reveals Pro-Kremlin Web Campaign', *Global Voices*, 13 July 2015.

[74] Agarwal, Nitin et al., 'BlogTrackers: A Tool for Sociologists to Track and Analyze Blogosphere'. (ICWSM, Citeseer, 2009).

This study can inform research conducted in the realm of 'antisocial computing'. Our findings will help counter the use of bots for propaganda: 1) by developing more efficient bot detection tools through continuously studying their evolving behaviours, so that these behaviours could be reported to Twitter in a timely fashion 2) by developing bots that target the same audience as our adversaries' bots do, study their narratives, and develop and massively disseminate counter-narratives to bury the messages of the adversary and 3) most importantly, by advancing our understanding of the information actors and their tactics in the new strategic communications environment.

Acknowledgments

This research is funded in part by the U.S. National Science Foundation (IIS-1110868 and ACI-1429160), U.S. Office of Naval Research (N000141010091, N000141410489, N0001415P1187, N000141612016, and N000141612412), US Air Force Research Lab, US Army Research Office (W911NF-16-1-0189), US 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.

Bibliography

Abokhodair, Norah, Daisy Yoo, and David 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*, 839–851.

Ackerman, Mark S., Jack Muramatsu, and David W. McDonald, 'Social Regulation in an Online Game: Uncovering the Problematics of Code', in *Proceedings of the 16th ACM International Conference on Supporting Group Work*, 173–182. ACM, 2010.

Agarwal, Nitin, Shamanth Kumar, Huan Liu, and Mark Woodward, 'BlogTrackers: A Tool for Sociologists to Track and Analyze Blogosphere', 2009.

Alexander, Lawrence, 'Open-Source Information Reveals Pro-Kremlin Web Campaign', *Global Voices*, 13 July 2015.

Al-khateeb, Samer, and Nitin 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.

Al-khateeb, Samer and Nitin Agarwal,'Examining Botnet Behaviors for Propaganda Dissemination: A Case Study of ISIL's Beheading Videos-Based Propaganda', 51–57. IEEE International Conference on Data Mining Workshop, 2015.

Al-khateeb, Samer, Kevin J. Conlan, Nitin Agarwal, Ibrahim Baggili, and Frank Breitinger,'Exploring Deviant Hacker Networks (DHN) On Social Media Platforms', *The Journal of Digital Forensics, Security and Law: JDFSL* 11, no. 2 (2016): 7–20.

Allen, Michael,'Kremlin's 'Social Media Takeover': Cold War Tactics Fuel Ukraine Crisis' *Democracy Digest, , National Endowment for Democracy*, 10 March 2014.

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

Blondel, Vincent D, Jean-Loup Guillaume, Renaud Lambiotte, and Etienne Lefebvre, 'Fast Unfolding of Communities in Large Networks' *Journal of Statistical Mechanics: Theory and Experiment* 2008, no. 10 (2008): P10008.

Bohlen, Celestine,'Cold War Media Tactics Fuel Ukraine Crisis' *The Times*, 10 March 2014.

Boshmaf, Yazan, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu,'Key Challenges in Defending against Malicious Socialbots', In *Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats*, 12–12. USENIX Association, 2012.

Brooking, T. Emerson, and P.W Singer,'War Goes Viral: How Social Media Is Being Weaponized across the World', *The Atlantic*, November 2016.

Cheng, Alex, and Mark Evans,'Inside Twitter An In-Depth Look at the 5% of Most Active Users', Sysomos Inc., 2009.

De Castella, Tom,'Malaysia Airlines MH370: The Persistence of Conspiracy Theories', *BBC News*, 8 September 2014.

Dewey, Caitlin,'A Comprehensive Guide to the Web's Many MH17 Conspiracy Theories', *The Washington Post*, 18 July 2014.

DoD News, Defense Media Activity,'Operation Atlantic Resolve Exercises Begin in Eastern Europe', 24 March 2015.

TV7 Israel News,'ISIL Executes an Israeli Arab after Accusing Him of Been an Israeli Spy', *TV7 Israel News*, 11 March 2015.

Ferrara, Emilio, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini,'The Rise of Social Bots', *Communications of the ACM* 59, no. 7 (June 24, 2016): 96–104.

Ghosh, Saptarshi, Bimal Viswanath, Farshad Kooti, Naveen Kumar Sharma, Gautam Korlam, Fabricio Benevenuto, Niloy Ganguly, and Krishna Phani Gummadi,'Understanding and Combating Link Farming in the Twitter Social Network', in *Proceedings of the 21st International Conference on World Wide Web*, 61–70. ACM, 2012.

Girvan, M., and M. E. J. Newman,'Community Structure in Social and Biological Networks', *Proceedings of the National Academy of Science of the United States of America* 99, no. 12 (6 April 2002): 7821–26.

Hegelich, Simon, and Dietmar Janetzko,'Are Social Bots on Twitter Political Actors? Empirical Evidence from a Ukrainian Social Botnet', In *Tenth International AAAI Conference on Web and Social Media*, 579–82. Cologne, Germany: AAAI, 2016.

Helton, Shawn,'Flight MH17 Conjures MH370, Exposing Western Deception, Leading To More Questions' *21st Century Wire*, 19 July 2014.

Holt, Thomas J.,'Examining the Forces Shaping Cybercrime Markets Online', *Social Science Computer Review* 31, no. 2 (2013): 165–77.

Howard, Philip N, Aiden Duffy, Deen Freelon, Muzammil M Hussain, Will Mari, and Marwa Mazaid,'Opening Closed Regimes: What Was the Role of Social Media during the Arab Spring? ', *Social Science Research Networks*, 17 April 2015.

Jaccard, Paul,'The Distribution of the Flora in the Alpine Zone', *New Phytologist* 11, no. 2 (1912): 37–50.

Jerome, Sara,'Ukraine-Russia Conflict Results In 'Water War' ', *Water Online*, 4 August 2014.

Karasaridis, Anestis, Brian Rexroad, and David Hoeflin,'Wide-Scale Botnet Detection and Characterization', in *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets*, Vol. 7. Cambridge, MA, 2007.

Kumar, Shamanth, Geoffrey Barbier, Mohammad Ali Abbasi, and Huan Liu,'TweetTracker: An Analysis Tool for Humanitarian and Disaster Relief', In *ICWSM*, 2011.

Labatut, Vincent, Nicolas Dugue, and Anthony Perez,'Identifying the Community Roles of Social Capitalists in the Twitter Network', 8. China, 2014.

Lutz, Catherine,'Is Social Media a Dangerous Force Against Democracy?', *The Aspen Idea Blog*, 6 August 2014.

Macfarguhar, Neil,'Aid Elusive, Crimea Farms Face Hurdles', *The New York Times*, 7 July 2014.

'Maltego', *Paterva A New Train of Thought*.

Moore, Sue,'The Economist - Worldwide Brand Report', *The Economist*, 8 November 2016.

Pavlishak, Alexel,'Water Supply Problem in Crimea to Cost $247- 417 Million - Kremlin Aide', *TASS Russian News Agency*, 28 April 2014.

Povar, Digambar, and V.K. Bhadran,'Forensic Data Carving', in *Digital Forensics and Cyber Crime*, 53:137–48. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer Berlin Heidelberg, 2011.

Preiss, Danielle,'How Social Media Is Helping Nepal Rebuild after Two Big Earthquakes', *Quartz India*, 19 May 2015.

Protalinski, Emil,'Facebook: 5-6% of Accounts Are Fake', *ZDNet*, 8 March 2012.

Reidy, Padraig,'MH17: Five of the Most Bizarre Conspiracy Theories', *The Guardian*, 22 July 2014.

Rodríguez-Gómez, Rafael A., Gabriel Maciá-Fernández, and Pedro García-Teodoro,'Survey and Taxonomy of Botnet Research through Life-Cycle', *ACM Computing Surveys (CSUR)* 45, no. 4 (2013): 45.

Schmidt, Charles W. 'Trending Now: Using Social Media to Predict and Track Disease Outbreaks." *Environ Health Perspect* 120, no. 1 (2012): 30–33.

Seddon, Max,'How A British Blogger Became An Unlikely Star Of The Ukraine Conflict — And Russia Today', *BuzzFeed News*, 20 May 2014.

Sen, Fatih, Rolf Wigand, Nitin Agarwal, Serpil Yuce, and Rafal Kasprzykm,'Focal Structures Analysis: Identifying Influential Sets of Individuals in a Social Network', *Social Networks Analysis and Mining* 6 (2016): 1–22.

Sen, Fatih, Rolf T Wigand, Nitin Agarwal, Mutlu Mete, and Rafal Kasprzyk, 'Focal Structure Analysis in Large Biological Networks', In *IPCBEE*, Vol. 70. 1. Singapore: IACSIT Press, 2014.

Shaheen, Kareem,'Isis Video Purports to Show Massacre of Two Groups of Ethiopian Christians', *The Guardian*, 19 April 2015.

Shirky, Clay,'The Political Power of Social Media: Technology, the Public Sphere, and Political Change', *Council on Foreign Relations* 90, no. 1 (February 2011): 28–41.

Sindelar, Daisy,'The Kremlin's Troll Army: Moscow Is Financing Legions of pro-Russia Internet Commenters. But How Much Do They Matter?', *The Atlantic*, 12 August 2014.

Smith, Craig,'By The Numbers: 170+ Amazing Twitter Statistics', *DMR (Digital Marketing Ramblings)*, 30 April 2016.

Smith, Marc A., Ben Shneiderman, Natasa Milic-Frayling, Eduarda Mendes Rodrigues, Vladimir Barash, Cody Dunne, Tony Capone, Adam Perer, and Eric Gleave, 'Analyzing (Social Media) Networks with NodeXL', in *Proceedings of the Fourth International Conference on Communities and Technologies*, 255–264. ACM, 2009.

Staff, BBC News,'Russia Fears Crimea Water Shortage as Supply Drops', *BBC News*, 25 April 2014.

Staff, CNN, 'ISIS Video Appears to Show Beheadings of Egyptian Coptic Christians in Libya', *CNN*, 16 February 2015.

Staff, DMR,'By The Numbers: 200 Surprising Facebook Statistics (April 2016)', *DMR (Digital Marketing Ramblings)*, 1 June 2016.

Staff, The Economist,'Russia, MH17 and the West A Web of Lies', *The Economist*, 26 July 2014.

Staff, Global Crime,'Exploring the Social Organisation and Structure of Stolen Data Markets', *Global Crime* 14, no. 2–3 (2013): 155–74.

Staff, Global Research,'Flight MH17 Conjures MH370, Exposing Western Deception, Was It a Staged Event? ', *Global Research*, 19 July 2014.

Staff, NPR,'The Arab Spring: A Year Of Revolution', *National Public Radio (NPR)*. 17 December 2011, All Things Considered.

Staff, Radio Free Europe,'U.S. Convoy: In Czech Republic, Real-Life Supporters Outnumber Virtual Opponents', *Radio Free Europe Radio Liberty*, 30 March 2015.

Staff, RT,"Tanks? No Thanks!': Czechs Unhappy about US Military Convoy Crossing Country', *RT Question More*, March 22, 2015.

Staff, RT,'Ukraine Builds Dam Cutting off Crimea Water Supply', *RT Question More*, 10 May 2014.

Staff, Sputnik,'Czechs Plan Multiple Protests Of US Army's Operation Dragoon Ride', *Sputnik News*, 2 March 2015.

Tatham, S. A., Defence Academy of the United Kingdom, and Advanced Research and Assessment Group. *Strategic Communication: A Primer*. Shrivenham: Defence Academy of the United Kingdom, Advanced Research and Assessment Group, 2008.

Yuce, Serpil, Nitin Agarwal, Rolf T Wigand, Merlyna Lim, and Rebecca S Robinson, 'Studying the Evolution of Online Collective Action: Saudi Arabian Women's 'Oct26Driving' Twitter Campaign', In *Social Computing, Behavioral-Cultural Modeling and Prediction*, 413–20. Springer, 2014.