National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

#WAR: THE WEAPONIZATION OF BOTNETS FOR ONLINE INFLUENCE ACTIVITIES

Major Matthew Johns

JCSP 45

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 45

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

#WAR: THE WEAPONIZATION OF BOTNETS FOR ONLINE INFLUENCE ACTIVITIES

Major Matthew Johns

Word Count: 5309

Nombre de mots : 5309

#WAR: The Weaponization of Botnets for Online Influence Activities

INTRODUCTION

'Fake news', 'going viral', 'retweets are not endorsements', 'one like = one prayer', '#FreeMosul', 'ratioed': in many ways these seemingly innocuous terms have become the new language of society, politics, and warfare. The rapid expansion of Web 2.0 and its associated social media platforms is driving a fundamental shift in how societies function and therefore how humans will wage war.[1] This change is tectonic in magnitude and reflects the global reach of platforms such as Facebook, Twitter, and YouTube. As David Patrikarakos notes in *War in 140 Characters*:

> …around 3.4 billion people now use the internet. Each day they send roughly 500 million tweets and upload nearly seven hours of footage to YouTube per second…Facebook has 1.7 billion active users, giving it a larger 'population' than China.[2]

In many cases, these new media have overtaken traditional government- or industry-controlled information services to become a dominant method of communication.[3] We are now challenged by the sheer amount of available data and human interaction, which arguably compromises our ability to categorize and trust it.[4]

---

[1] P.W. Singer & Emerson T. Brooking, *Likewar: The Weaponization of Social Media.* (New York : Houghton Mifflin Harcourt, 2018), 45. Web 2.0 is a term used to define the move towards a more graphically interfaced and user-controlled experience of the Word Wide Web and away from the more text-based interfaces of the early internet. This change is generally identified as beginning slowly in 2001 with the creation of Wikipedia, but expanding rapidly with the introduction of graphic interface social media platforms such as Facebook, Twitter, and YouTube.

[2] David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century*. (New York : Basic Books, 2017), 8.

[3] *Ibid*, 9.

[4] Xianchao Zhang, Shaoping Zhu & Wenxin Liang, "Detecting Spam and Promoting Campaigns in the Twitter Social Network" in *Record of the 2012 IEEE 12th International Conference on Data Mining.* (Washington DC : IEEE Computer Society, 2012), 1194.

Problem Background

No longer do nations have the monopoly on control of information to their citizens, which has broadened the traditional window of opportunity for influence activities by both state and non-state actors to impose their will on perceived enemies and their civilian populations.[5] This is of critical concern as the strength of popular will and public unity are of paramount importance to military operations and good governance.[6] This centrality is noted by the Department of National Defence (DND) which states "the moral component is concerned with the persuasion of people to fight and recognizes that it is people who realize military power."[7] Unfortunately, many pluralistic Western states remain extremely vulnerable to these influence activities.[8] The magnitude and complexity of the problem has meant that many governments simply do not seem capable of addressing the threat, as the Communications Security Establishment (CSE) identifies about Canada.[9]

One of the most pernicious and effective methods of influencing populations is through the targeted use of botnets; digital systems which can be used to propagate

---

[5] Keir Giles, *Handbook of Russian Information Warfare.* (Rome : NATO Defence College, 2016), 6. Broadly speaking these efforts are captured under the term influence activities that includes psychological operations, strategic communications, influence and disinformation that forms "a whole of systems, methods and tasks to influence the perception and behaviour of the enemy, population, and international community on all levels."

[6] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security.* 38:2: 7-8.

[7] Department of National Defence, *CFJP 01 Canadian Military Doctrine.* (Ottawa : Department of National Defence, 2009), 2-3.

[8] Congress of the United States, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security.* (Washington D.C. : Committee on Foreign Relations United States Senate, 2018), 9.

[9] Communications Security Establishment, *Cyber Threats to Canada's Democratic Process.* (Ottawa : Communications Security Establishment, 2019), 32-33. CSE outlines significant threats to the next (2019) Federal election, identifying that it is likely that organized states, but also corrupt non-state actors, will seek to use digital influence tools to shape the electoral process.

messages by amplifying their reach.[10] This method will continue to gain traction as it becomes an ever more affordable and effective tactic for conducting psychological operations.[11] Examples are as diverse as Russian interference in the 2016 United States (US) election[12] or the Islamic State's (IS) use of botnets for both recruiting and terror tactics.[13] These cyber-amplified voices drown out counter-narratives and undermine legitimate government and military attempts to "get the truth out".

This paper contends that the Canadian Armed Forces (CAF) remains unprepared to address the threat posed by botnet enabled influence activities, and this puts it at risk of conceding the moral plane in operations.[14] To address this deficiency, the CAF must systematically identify means of expanding its online reach in order to counter effective enemy influence operations. Specifically, the CAF must address the rapid proliferation of such operations across the cyber domain, the most effective manner in which is the employment of CAF controlled botnet systems to amplify messaging and extend digital reach. This work will identify the requirement by demonstrating the impacts of adversary influence activities enabled through botnets and our current inability to counter them. Subsequently, the feasibility of establishing a botnet for influence activities and the potential option space for the CAF will be explored. Finally, this paper will identify

---

[10] Vera Zakem, Megan K. McBride & Kate Hammerberg, *Exploring the Utility of Memes for U.S. Government Influence Campaigns.* (Arlington : CNA Analysis & Solutions, 2018), 29.

[11] David Carment & Dani Belo, "War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare." Last accessed 1 May 2019, https:www.cgai.ca.wars_future_the_risks_ and_rewards_of_grey_zone_conflict_and_hybrid_warfare. Beyond affordability the nature of influence activities conducted in the cyber domain is the deniability they provide. Difficulties in attribution mean that nation states can often leverage these capabilities "in the margins" of conflict.

[12] Robert S. Mueller, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election, Volume I of II.* (Washington DC : United States Department of Justice, 2019), 4.

[13] Singer & Brooking, *Likewar*, 5.

[14] Ryan Clow, "Psychological Operations: The Need to Understand the Psychological Plane of Warfare." *Canadian Military Journal*. 9 (1), 24.

potential concerns surrounding the employment of such technology and areas for future investigation.

THE REQUIREMENT

Web 2.0 has driven an enormous growth in online activity that has fundamentally realigned our structures of communications, information control, narrative perspective and, arguably, truth.[15] The global reach of internet communications, coupled with its ability to flatten communications chains and link up disparate participants has altered pre-existing standards. The nature of the internet makes attribution, the ability to assign responsibility for an action to a specific state or person, almost impossible.[16] This combination of reach, obfuscation, and influence means that a sufficiently "loud" message can permeate Web 2.0 systems with rapidity, what is generally termed "going viral".[17]

The ability to go viral is critical to propagating information operations across the web. The most insidious and effective method for ensuring rapid growth of a message is amplification through botnets.[18] Botnets are centrally controlled groupings of computers or networks that are generally tailored for specific activity, coordinated through

---

[15] Computational Propaganda Project. "Resource for Understanding Political Bots." Last accessed 5 April 2019, https://comprop.oii.ox.ac.uk/research/public-scholarship/resource-for-understanding-political-bots/

[16] Kello, "The Meaning of the Cyber Revolution," 32.

[17] Singer & Brooking, *Likewar*, 173.

[18] Clint Watts, "Clint Watts' Testimony: Inside Russia's Fake News Playbook." Last accessed 30 April 2019, https://www.thedailybeast.com/inside-russias-fake-news-playbook. Clint Watts is a former FBI agent who served in the counter-terrorism and national security branches. He has made multiple appearances before Congress (both House and Senate) with regards to intelligence and security matters.

command and control software.[19] These distributed groupings can then be used *en masse* to conduct specified tasks such as distributed denial of service (DDOS) or the spread of malware.[20] A more recent development with regards to the employment of botnets is its targeted used in the amplification and spreading of misinformation and propaganda as a means of shaping discourse and sowing discord.[21] In this case, a botnet is controlled by an individual or organization and pushes a particular narrative in service to its controller, often across a wide spectrum of social media platforms such as Twitter, YouTube, and Facebook. By creating the perception of broad-based support, created through rapid propagation of "likes" and "shares" artificially generated by the botnet, the algorithms of social media platforms amplify desired messaging.[22] Adversaries, whether asymmetric threats from non-state actors or traditional great power "grey zone" competition[23], have actively pursued psychological influence operations through propaganda and the coordinated use of botnets.[24] The ability of adversaries to leverage these technologies to enhance their influence operations is well documented and poses a serious threat to the Government of Canada and to the CAF's ability to prosecute operations in the cognitive

---

[19] Felix Brezo, Jose Gaviria De La Puerta, Igor Santos & David Barroso. "C&C Techniques in Botnet Development" in *International Joint Conference CISIS 12-ICEUTE Special Sessions.* (Seville : CISIS, 2012), 2-3.

[20] Jinxue Zhang, Rui Zhang, Yanchao Zhang & Guanhua Yan. "The Rise of Social Botnets: Attacks and Countermeasures." *IEEE transactions on Dependable and Secure Computing.* 15(6): 1068-1069.

[21] Erin Gallagher, "Propaganda Botnets on Social Media." Last accessed 28 April 2019, https://medium.com/erin_gallagher/propaganda-botnets-on-social-media-5afd35e94725. Because botnets can be used to amplify messages and concepts they can be leveraged to introduce problematic messaging into debates and then rapidly boost the signal strength of weak signals. This is a highly effective method of increasing disinformation and division within a community.

[22] J.M. Berger, "How ISIS games Twitter." Last accessed 28 April 2019, https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

[23] Carment & Belo, "War's Future."

[24] Patrikarakos, *War in 140 Characters,* 264-265.

domain.[25] Two examples of this threat, one asymmetric and one state based, will be explored to elaborate on the dangers posed to our current capabilities.

Crowd-sourcing terrorism: The Example of IS

The meteoric rise to infamy of IS is almost directly attributable to its effective use of social media to rapidly establish itself as a "brand" online.[26] Through a combination of infamous brutality and extremely clever marketing, the terrorist organization became a global phenomenon almost overnight. There can be no doubt that much of this was accomplished through aggressive online marketing and well-produced videos and imagery that were shared broadly across YouTube and Instagram.[27] However, this explosive growth is also a testament to IS' ability to take advantage of available systems for "hacking" social media, leveraging tools as such as botnets to grossly enhance its initial impact.[28] This "market penetration" ensured that it could focus attention on its online presence and thus drive the narrative, establishing IS as a global organization.[29]

This broad reach allowed IS to fundamentally shape the ongoing narrative surrounding its activities and to seek out support for combatants, funding, and other materiel. By achieving saturation of the social media ecosystem, IS was able to "crowd-source" terrorism across the world, by either drawing adherents to the region or

---

[25] Communications Security Establishment, *Cyber Threats to Canada's Democratic Process,* 20.

[26] Emerson T. Brooking & P.W. Singer, "War Goes Viral." Last accessed 27 April 2019, https:/www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/

[27] Singer & Brooking, *Likewar*, 152. IS launched its cause in 2014 using the viral hashtag #AllEyesonISIS. They subsequently identified other viral or popular hashtags, such as ones related to the World Cup and coopted them with IS messaging to broaden their reach.

[28] Zhang, Zhang, Zhang & Yan. "The Rise of Social Botnets," 1068-1069.

[29] Zhang, Zhu & Liang, "Detecting Spam and Promoting Campaigns in the Twitter Social Network" 1194-1195.

radicalizing individuals and groups to strike in the homelands of those opposed to IS.[30] This rapid promulgation of ideology and operations was unprecedented, representing a significant break from the types of online operations conducted by terrorist organizations in the past.[31] IS embraced Web 2.0, arguably as the first digitally-enabled, social network-centric terrorist group[32], and are considered "the first terrorist group to hold both physical and digital territory."[33]

Recognizing that as a non-state actor it faced considerable limitations in terms of personnel, equipment, and funding, IS turned to the burgeoning world of social media and weaponized it like no one before. Leveraging effective and cheap communication systems, IS engaged with criminals to establish botnets[34], and simultaneously developed software to allow its supporters to broadcast its message, effectively turning humans into an organized botnet that retweeted imagery and messages in support of IS. By launching their war with the hashtag #AllEyesOnISIS they leveraged fear by sharing horrific imagery which undermined the Iraqi garrison's will to fight:

> The Iraqi army stood ready to protect the city from this tiny but fearsome horde - in theory, at least…Worse, the roughly 10,000 who actually did exist were able to track the invading army's highly publicized advance and atrocities on their smartphones. With #AllEyesOnISIS soldiers began to ask each other if they should fight or flee. The enemy hadn't even arrived, but fear already ruled the ranks.[35]

At its peak, IS' apps were generating up to 40,000 individual tweets a day in support of

---

[30] Singer & Brooking, *Likewar*, 9.

[31] Patrikarakos, *War in 140 Characters,* 209.

[32] *Ibid,* 230.

[33] Brooking & Singer, "War Goes Viral."

[34] Virginia Regester, *an Assessment of Botnets as an Offensive Cyber Weapon for the United States.* (New York : Utica College, 2015), 41.

[35] Singer & Brooking, *Likewar*, 6.

their actions; tweets that would subsequently be liked and retweeted by human and bot alike, continuing to amplify the message.[36] IS simply overwhelmed any counter-narrative by shouting it down through bot enabled retweets, gaming the social media algorithms that identify popular trends and projecting its own to dominance across the information domain.[37] A clear example of this: following the capture of Mosul in 2014, IS began a social media campaign threatening the Iraqi capital of Baghdad with images of IS fighters and the online threat "we are coming Baghdad". The ability to rapidly rebroadcast this message and saturate the social media ecosystem meant that within hours the image of IS fighters became one of the first results of searches for the term "Baghdad."[38]

At its peak, IS was a formidable force in the physical and cyber domains, but it was still ultimately an asymmetric threat and its activities in the Web 2.0 ecosystem reflect this reality. Unlike a more resourced symmetric adversary such as Russia, IS was not focused on subversion and working within the "grey zone" of legally dubious activity.[39] Instead, unconstrained by the strictures of international law and public perception, it became in effect the greatest "troll army" seen in social media, with a cache on content that could generate up to 1,000 media releases a month.[40] IS' presence was so pervasive and dominating that many of its online fans began to refer to its social media presence as *wilayat Twitter* (the state of Twitter).[41] Yet, by comparison it was still a

---

[36] Berger, "How ISIS games Twitter."
[37] Patrikarakos, *War in 140 Characters,* 205.
[38] Berger, "How ISIS games Twitter."
[39] Carment & Belo, "War's Future."
[40] Singer & Brooking, *Likewar*, 152-153.
[41] Patrikarakos, *War in 140 Characters,* 232.

relatively small organization that was greatly enabled in the spreading of digital jihad through the extensive use of modern social media technology, one example being its use of botnets to re-tweet and share messages that had been identified with its preferred hashtag.

Although pervasive and in many ways highly effective, IS was not subtle.[42] IS effectively brought terrorism to the internet and leveraged its botnets using the same approach it used in the physical plane. In effect, IS used brute force to enhance their online numbers to simply shout down opposition and drown out debate.[43] What IS did not do was attempt to fundamentally reshape the order and social cohesion of perceived adversaries; it did not traffic in misinformation so much as self-aggrandizing propaganda. IS did not seek to sow discord amongst its enemies – it simply targeted them for destruction and leveraged its social media capabilities to sow terror.

Fake News and Culture Wars: The Example of Russia

The more insidious use of botnets to subtly shape public discourse is reserved for states with more resources, such as Russia. Russia, and its predecessor the Soviet Union, has a history of engaging in long-term manipulation and disinformation campaigns aimed at undermining the unity and stability of adversary states.[44] Described in various terms such as "active measures", *maskirovka* (strategic deception), and *dezinfortmatsiya*

[42] Berger, "How ISIS Games Twitter." The hashtag (#) is the internet's short form for identifying a topic or subject. By appending text after the # symbol web crawlers and platforms such as Twitter and Instagram identify the following term as a searchable/grouped topic. Examples include #WorldCup and #ABElection. Twitter aggregates discussions based on the number of times a particular hashtag appears, if it is sufficiently retweeted it will be added to the @ActiveHashtags account and subsequently rebroadcast, thus enhancing vitality and reach. IS was particularly adept at brute forcing the vitality of their hashtags by using botnets to retweet them over and over.

[43] Patrikarakos, *War in 140 Characters,* 240.

[44] Giles, *Handbook of Russian Information Warfare,* 3.

(disinformation), these efforts have spanned the history of Soviet and Russian efforts to counter-balance the perceived threat from Western nations.[45] Where before Russian propaganda and disinformation might have been planted months in advance in various newspapers and allowed to gradually develop, with the power of social media and botnets Russian misinformation can effectively be "shotgunned" into the Web 2.0 ecosystem with rapid fire intensity.[46] Through a combination of blatant propaganda (fake news), misinformation, and manipulation of partisan emotions – all supported by aggressive botnet systems – Russian influence operations in cyberspace have transcended the old forms of *maskirovka* and *dezinformatsiya*.[47]

Today, the democracies of the Western world face the threat of the "Gerasimov Doctrine", a strategic approach to leverage the low cost and potentially high payoff of social media information operations.[48] The reach and penetration of social media into the daily lives of adversary state citizens means that Russia can bring its disruptive efforts directly into the homes of its enemies. In contrast to the "swagger" of IS, the majority of Russian influence operations are comparatively subtle, focused on leveraging pre-existing conflicts within populations to sow discord and reduce social cohesion.[49] Russia sees such efforts as a low cost/risk, potentially high payoff method of achieving overmatch in

---

[45] Congress of the United States, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security.* (Washington D.C. : Committee on Foreign Relations United States Senate, 2018), 35-36. It must be clear that recent Russia efforts at disinformation are not a new development but wholly inline with previous Soviet doctrine. What is new is Russia's leveraging of emerging technologies to better disseminate disinformation in support of influence operations.

[46] Marcus Kolga, *Stemming the Virus: Understanding and Responding to the Threat of Russian Disinformation.* (Toronto : Macdonald-Laurier Institue, 2019), 21.

[47] Mueller, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election, Volume I of II*, 1-2.

[48] Giles, *Handbook of Russian Information Warfare,* 64.

[49] Singer & Brooking, *Likewar*, 206.

the information domain, and thus, as laying the groundwork for a potential shift to the existing global order.[50] Recognizing the inherently asymmetric nature of their relationship with adversaries such as the North Atlantic Treaty Organization (NATO) and the US, the Russian government has instead opted to wage undeclared psychological operations in the "grey zone", where legality is dubious and attribution difficult.[51] This is a distinctly different methodology than IS practices, but it is just as dangerous, if not more, due to its insidious nature. IS may shout from the internet rooftops, but their propaganda remains clearly self-serving and obvious. By contrast, influence operations conducted by Russia in the cyber domain run the gamut from obvious propaganda to subtle misinformation disguised as legitimate, all paired with actors in the real world like the activist Mariia Butina.[52]

It is well documented that Russia has engaged in influence operations against multiple adversaries[53] and is further likely to continue to do so, including activities targeting Canada.[54] However, in the public consciousness these actions pale in comparison to those undertaken to influence the US election of 2016.[55] In this case, Russia deployed its complete arsenal of influence operations capabilities, most notably its

---

[50] Communications Security Establishment, *Cyber Threats to Canada's Democratic Process,* 12-13.

[51] Kolga, *Stemming the Virus,*13-14.

[52] United States Department of Justice, *Affidavit in Support of an Application for a Criminal Complaint for Mariia Butina*. (Washington D.C. : District Court for the District of Columbia, 2018), 4-5. Butina acted as an unregistered foreign agent in the US. Under the guise of promoting gun ownership rights in Russia she pursued relationships with senior leaders in the National Rifle Association (NRA) and associated leaders in government. Gun rights remains a highly contentions issue in the US and her involvement was evaluated as an effort to further stop conflict.

[53] Paul Szoldra, "Military Leaders are Starting to freak Out Over Russia's Information Warfare Dominance." Last accessed 22 April 2019, https://taskandpurpose.com/russia-information-war

[54] Communications Security Establishment, *Cyber Threats to Canada's Democratic Process,* 12-13.

[55] Mueller, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election, Volume I of II*, 1-2.

"troll factory" managed by the Internet Research Agency (IRA) – a Russian botnet organization.[56]

In many ways, the IRA defines the concept of weaponized social media: an organization with a broad mandate who conducts activities across the spectrum of conflict. In 2016, its operatives were engaged in targeting social media adversaries in Ukraine while simultaneously masquerading as social justice advocates in the US.[57] Their messaging was supported and amplified by an aggressive network of botnets and "sockpuppets" to push their narrative into the Web 2.0 ecosystem[58] while pretending to be trusted news sources or political groups. For example, @TEN_GOP was a Russian sock puppet account and not the Tennessee Republican party. IRA would use these accounts to sow division amongst antagonistic parties in the US, leveraging the so-called "culture wars" primarily.[59]

The IRA networked its operatives, giving them detailed direction on what, who, and how to target various adversaries. They developed coordinated teams who were provided with detailed background information and directed to create "political intensity through supporting radical groups, users dissatisfied with [the] social and economic

---

[56] United States Department of Justice, *United States v. Internet Research Agency et al.* (Washington D.C. : District Court for the District of Columbia, 2018), 3-4.

[57] Giles, *Handbook of Russian Information Warfare,* 54.

[58] Watts, "Clint Watts' Testimony." A sockpuppet is a fake identity established on the internet. It is generally used as an "alternate voice" to support a particular argument. Thus, if engaged in a debate one of the debaters would switch to a sockpuppet account and comment on the debate, providing the perception of additional support for an idea. Much like botnets this can be leveraged to build the appearance of consensus and support.

[59] Giles, *Handbook of Russian Information Warfare,* 47. Culture wars is a US-centric term that reflects stark divisions in US society over issues such as abortion, religion, and gun ownership.

situation and oppositional social movements."[60] This established a self-reinforcing system that created messages, injected them into the heated debate surrounding the US election, and amplified these narratives to stoke division. By seizing on a particularly contentious issue, such as the Black Lives Matter movement, Russian operatives could insert incendiary comments into a discussion, and then re-tweet and share it through their botnets to fan the flames.[61] These efforts at manipulation were highly successful and demonstrated the efficacy of botnet activities such as "click fraud" – the appearance of consensus in social media – through amplification and narrative control.[62] Several near-riots were incited when Russian operatives surreptitiously coordinated protests and counter-protests by rival groups to occur simultaneously.[63]

To achieve this level of influence, the Russian government, controlling the IRA through the plausible deniability of internet anonymity, directed and managed the activity of at least 3,814 Twitter accounts. These accounts sent over 175,000 tweets reaching at least 1.4 million users in a ten-week period prior to the US election.[64] The IRA also took to actively reinforcing these messages with aggressive purchasing of advertisements on other social media platforms such as Facebook.[65] Once again, Russia leveraged their ability to unify their influence operations activities through the IRA. Messages that were positively received on Twitter were subsequently amplified through botnets to achieve

---

[60] United States Department of Justice, *United States v. Internet Research Agency et al.* (Washington D.C. : District Court for the District of Columbia, 2018), 14.

[61] *Ibid,* 14.

[62] Gallagher, "Propaganda Botnets on Social Media."

[63] Singer & Brooking, *Likewar*, 114-115.

[64] Mueller, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election, Volume I of II*, 28.

[65] United States Department of Justice, *United States v. Internet Research Agency et al.* (Washington D.C. : District Court for the District of Columbia, 2018), 14.

vitality and then, when adopted by targeted US groups as their own, further amplified by targeted advertisements.[66] This led to specific messages in IRA-controlled groups reaching up to 4 million people with over 300,000 likes and shares.[67]

Although many of the Russian efforts were not subtle (i.e., they had a tendency to be active starting at 0800 hours Saint Petersburg time), they were not nearly as blatant as those conducted by IS and so were accepted as legitimate voices in the debate.[68] Russian influence operations conducted through the IRA demonstrated an appreciation for a long-term strategy focused on the gradual and subtle erosion of social cohesion within targeted adversaries. A prime example is the establishment of Twitter user @Jenn_Abrams, played as a "sassy American teen" who was active in all manner of discussion from pop culture to Donald Trump.[69] By skillful manipulation of botnet support initially, @Jenn_Abrams built a following of nearly 70,000 users. The virility of the account led to it being quoted across the spectrum of American media, which subsequently led to yet more spreading of the viral messages designed by the IRA.[70]

The carefully arranged approach of the IRA reflects the tradition of Russian *dezinformatsiya* and demonstrates the threat posed by influence operations in social media. These methods led to a breakdown in communication in the US and the further polarization of citizens, and demonstrated a profound long-term understanding of

---

[66] *Ibid,* 27.

[67] Singer & Brooking, *Likewar*, 114.

[68] Patrikarakos, *War in 140 Characters,* 149-150. Beyond time zones and suspiciously synchronized activity many bots and sockpuppets were identified by astute online observers based on their poor use of english and tendency to push a recurring phrase or message.

[69] Mueller, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election, Volume I of II*, 27.

[70] Singer & Brooking, *Likewar*, 114.

strategic benefit by destabilizing a key adversary.[71] The efforts of Russian botnets and sockpuppets directly contributed to undermining the perceived legitimacy of news agencies and official government reporting, and continues to be debated today.[72] These influence operations advanced the Russian long-term goal of subverting existing global orders and overmatching in the information domain through the use of grey zone asymmetric efforts.[73]

We've Been Trolled: The Current State of Play

The threat posed to national and military structures by weaponized social media, specifically that supported by botnets, is severe.[74] As demonstrated, the impacts of aggressive social media influence operations can have real-world results, such as the fall of Mosul or the election of Donald Trump. The CAF has entered into this virtual arena significantly underarmed, a reflection of a general trend in Western democracies.[75] Although all Western nations and their militaries advocate for the primacy of the moral plane or the cognitive domain[76] as the critical battlespace, our efforts in the digital environment — the ecosystem where this domain is most accessible — remain hamstrung.[77]

This threat is certainly not contained only to Canada. The majority of our allies

---

[71] Kello, "The Meaning of the Cyber Revolution," 8.

[72] Singer & Brooking, *Likewar*, 113.

[73] Szoldra, "Military Leaders are Starting to freak Out Over Russia's Information Warfare Dominance."

[74] *Ibid.*

[75] Carment & Belo, "War's Future."

[76] Department of National Defence, *CFJP 01 Canadian Military Doctrine,* 3.

[77] Szoldra, "Military Leaders are Starting to freak Out Over Russia's Information Warfare Dominance."

face similar challenges with maintaining the pluralistic nature of their societies while unified adversaries leverage a spectrum of threats against them.[78] Nor is the threat merely a military one, as evidenced by outcomes in the US elections and continuing social unrest across Western nations. Addressing the national security threat posed by amplified social media is beyond the scope of this paper, but it is important to highlight that the CAF itself is operationally at risk due to this evolving threat.

Much of the CAF's difficulty stems from the Western approach to social media as a "marketplace of ideas", where the natural quality of truthful and strong narratives will win out.[79] Our current doctrine, as outlined in CANFORGENs and *Guidelines for the External Use of Social Media,* is outdated (2011) and unprepared to face the reality of a rapidly propagating, decentralized social media ecosystem. In previous eras, where national media and government controlled much of a society's access to information, this "forum of ideas" was likely true.[80] However, in the world of Web 2.0 it is not simply truthful narrative that will carry the day; dominance via technical means is crucial to success.[81] It is because of this lack of capability that the CAF risks being decisively overmatched in the social media domain, surrendering that battlespace to our adversaries.

The nature of Western military approaches to social media tends to reflect the conservative nature of the institutions involved; they inherently find themselves

---

[78] Carment & Belo, "War's Future."

[79] Assistant Deputy Minister Public Affairs, *DND/CF Guidelines for the External Use of Social Media.* (Ottawa : Department of National Defence, 2011), 4-5.

[80] Anthony Seaboyer, *Influence Techniques Using Social Media.* (Kingston : Defence Research and Development Canada, 2018), 2-3.

[81] Regester, *an Assessment of Botnets as an Offensive Cyber Weapon for the United States,* 42.

challenged in achieving reach even before technical concerns come into play.[82] For example, even at the peak of Operation LENTUS in the national capital region, tweets by the Chief of Defence Staff (CDS) in support of the operation only achieved on average 250 likes and barely a dozen retweets.[83] This was an operation that implicated several thousand troops in the nation's capital and yet the commander of the CAF could not achieve a narrative breakthrough in either official language. With our current capabilities and approach, it is not feasible that the CAF will be able to maintain a decisive advantage in the moral plane if social media is the battlespace of the future. At this time, it cannot control its narrative at home, much less on expeditionary operations where the need to combat potential terrorist messaging or grey zone conflict is even higher.

Arguments can be made for a requirement to modernize the entirety of the CAF's approach to social media, maximizing efforts to achieve vitality and narrative breakthrough, although addressing all these issues simultaneously would be challenging.[84] What is crucially relevant is the inability of the CAF to adequately broadcast its message to those it hopes to influence. The CDS has only 9,831 followers which, even if they were all members of the CAF itself, accounts for less than 15% of uniformed personnel.[85] Similarly, the @CFOperations Twitter account has 35,000

---

[82] Seaboyer, *Influence Techniques Using Social Media.* (Kingston : Defence Research and Development Canada, 2018), 11-12.

[83] Twitter. "Search results for CDS." Last accessed 2 May 2019, https://twitter.com/CDS_Canada_CEMD

[84] Janzen, Col Jay. *What if the Pen IS a Sword? Communicating in a Chaotic, Sensational, and Weaponized Information Environment.* (Toronto : Canadian Forces College, 2018), 1.

[85] Twitter. "Search results for CDS." Last accessed 2 May 2019, https://twitter.com/CDS_Canada_CEMD

followers across the globe but is only averaging a few dozen likes per tweet.[86] Undoubtedly, one of the most significant issues facing the CAF's influence operations on social media is its inability to reach its intended targets, either at home or abroad.

Expanding the CAF's social media reach is crucial to establishing its capability for influence operations going forward. If we are truly serious about competing in the social media domain, we must accept that, as with all domains, appropriate weapons must be utilized to achieve success. Enemies, both nation-state and asymmetric, have demonstrated a dangerous capacity to mobilize social media through influence operations; that threat must be recognized and, if not neutralized, at least mitigated.[87] A simple solution is the employment of friendly botnets for the amplification of messaging. While this paper will not dispute the importance of narrative truth and clarity, the criticality of reach and social media penetration must also be considered, or we surrender any military advantage to our adversaries.[88] We have entered a new age of influence warfare and the CAF has not modernized its weapon system to address emerging threats. It stands armed with its smoothbore musket, arrayed against a machine gun nest of botnets that can fill the air with counter-narrative in an instant.

FEASIBILITY

In order to ensure it is not made irrelevant in the social media domain the CAF must focus on re-arming itself for Web 2.0 battlespace. The crux of this rests on the ability to amplify the CAF's signal and reach those who are currently being cut off by

---

[86] Twitter. "Search results for CF Operations." Last accessed 2 May 2019, https://twitter.com/CFOperations

[87] Kello, "The Meaning of the Cyber Revolution," 12-13.

[88] Singer & Brooking, *Likewar*, 179.

adversary signals. Although there are many ways to increase virality, one of the simplest and most effective is by simply boosting the signal strength of the message.[89] Botnets provide a cheap and effective method of doing so and could be incorporated into CAF social media standards.

The Option Space

The quality of CAF messaging is often strong and contains many of the features which enhance the likelihood of virality: narrative, emotion, authenticity, and community. However, it consistently lacks one of the most critical elements: inundation.[90] This refrain is common in Western agencies; Alberto Fernandez, former coordinator of the Center for Strategic Counterterrorism Communications (CSCC), identified that the biggest challenge facing his office in its struggle against IS and al-Qaeda was not the quality of content, but ability to penetrate the social media ecosystem.[91] Again, amplification could be achieved easily through botnets.

Botnets are a cheap and effective system for operating within social media. Their relative lack of complexity allows for them to be centrally controlled and coordinated with little advanced infrastructure required.[92] The nature of botnets could allow for multiple approaches to their implementation and employment within the CAF, from a centralized system for domestic audiences (to maintain maximum control) to a de-

---

[89] Communications Security Establishment, *Cyber Threats to Canada's Democratic Process,* 20.

[90] Singer & Brooking, *Likewar*, 154.

[91] Patrikarakos, *War in 140 Characters,* 249. The CSCC was a small organization within the US State Department whose mandate was primarily anti-radicalization and counter-terrorist. It was a digitally focused section that sought to counter adversary online propaganda on social media with its own. Although it achieved some success due to its Arabic language use and clever approach it was generally overmatched by IS propaganda systems that could effectively "shout it down".

[92] Brezo, JDe La Puerta, Santos & Barroso. "C&C Techniques in Botnet Development," 2-3.

centralized or even peer-to-peer system abroad to effectively mask the effort from adversary detection.[93] As Zhang, Zhang, Zhang & Yan outlined in 2013, it is relatively simple to establish an effective botnet on Twitter; which if properly synchronized with other social media platforms, will ensure significant penetration of desired messages.[94] The benefit of varied approaches to botnet coordination is the ability to reorient it for both defensive (counter-narrative) and offensive (narrative) purposes, with the ability to obfuscate the origin if required.

Some of the most common complaints surrounding social media is the rapid dissemination of incorrect or false information, and specifically for the military, the slow response (if any) that is issued to correct such inaccuracies. To address "fake news" stories, the CAF could leverage a botnet system resident within Assistant Deputy Minister - Public Affairs or Director General Cyber; perhaps outside the CAF entirely but in service to the government. The distributed and ambiguous nature of internet communications allows flexibility, and the CAF must take advantage of this. The existence of a CAF botnet system could ensure the proper amplification of corrective messaging, to ensure that the truth makes it to the intended audience. *The Wavell Room*, a British military blog, expressed support for just such a concept. They argued "a separate Twitter account could challenge some of the fake news stories out there. It

---

[93] *Ibid,* 3-4.

[94] Zhang, Zhang, Zhang & Yan. "On the Impact of Social Botnets for Spam Distribution and Digital-Influence Manipulation" in *Record of the 2013 IEEE Conference on Communications and Network Security.* (Washington DC : IEEE Computer Society, 2013), 47.

could, through "Direct Messaging", offer an alternative."[95]

Direct messaging could also be a force multiplier in the context of expeditionary operations. Just as IS broke the will of the Iraqi army at Mosul with #AllEyesOnISIS, so too could CAF forces impose their will on adversaries abroad.[96] This is nothing new from the point of view of influence activities, but our current doctrine does not allow the CAF to fully leverage the power of social media to reach its enemies. Judicious use of the targeting process to identify key adversary actors, and then bombardment of their networks with targeted messaging could sap their will. Conversely, use of such a system to promote positive or helpful messages to local populations could be of tremendous help to a deployed organization. The number of social media users continues to grow exponentially, and the Web 2.0 must be considered as our primary means of communication in these contexts.[97] With a massive ecosystem to target, the CAF must consider automating some of these efforts.

Leveraging automated botnets for the promotion of messages and information is not a new phenomenon for Web 2.0 and is arguably one of its foundational structures, as it drives the algorithms which govern these social media spaces.[98] What is unique for CAF consideration is the employment of this method for the amplification of its own

---

[95] Gordon. "Winning the Narrative - An Army Officer's Perspective." Last accessed 1 May 2019, https://www.wavellroom.com/2018/07/05/how-do-you-win-the-narrative-utm_content=buffe r4aa3f&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer. It must be noted that *The Wavell Room* does not advocate for false Twitter accounts to share fake news within the UK, but in fact as a voice to counter it, either through reinforcement of messaging or by countering narratives in a more direct manner that formal military social media may not adopt.

[96] Singer & Brooking, *Likewar*, 152

[97] *Ibid,* 48.

[98] Zhang, Zhang, Zhang & Yan. "On the Impact of Social Botnets for Spam Distribution and Digital-Influence Manipulation", 46.

messages, whether domestically or abroad. This idea is not unique or new to the military; such a suggestion was explored as early as 2008 for the United States Air Force at the dawn of the Web 2.0 age.[99] Colonel Williamson III recognized that to oppose botnets, one likely required botnets. Although in his argument he focused on their potential use for DDOS attacks, it must be understood that the principal for social media amplification remains the same.[100] What Williamson had correctly identified is that the only way to combat the distributed, highly flexible and responsive nature of the networked threat was with a similarly empowered network.

This approach to network defeat was not unique to Williamson. John Herrmann, a David Carr fellow at *The New York Times* who specializes in social media, paraphrased General Stanley McChrystal:

> McChrystal noted that it takes a network to defeat a network. Propagandists use networks (social and fabricated such as botnets) to spread confusion and disinformation. It would be wise to develop a network to promote truth and counter falsehood.[101]

This paper does not advocate for a wholesale change to the influence operations conducted by the CAF, including its formal Public Affairs activity. The centrality of truth to the CAF's narrative must remain, but that does not mean that it cannot be amplified to ensure that it reaches the intended audiences for the purpose of promoting virality and message penetration.[102] This approach is crucial to enabling the CAF to

---

[99] Kevin Poulsen, "Air Force Colonel wants to build a military BotNet." Last accessed 20 April 2019, https://www.wired.com/2008/05/air-force-col-w/

[100] *Ibid.*

[101] John Herrmann, *'Truth': Why Spock is Such an Unusual Character.* (Phoenix : Weapon Narrative Initiative for the Center on the Future of War, 2017), 24.

[102] Zhang, Zhang, Zhang & Yan. "On the Impact of Social Botnets for Spam Distribution and Digital-Influence Manipulation," 46.

conduct future influence operations in that environment.

The potential value that botnets could provide the CAF for influence activities is significant. We face a serious threat from adversaries who are not constrained by our concerns about social media and have effectively weaponized it against us.[103] The CAF is crucially behind in the social media arms race and we must take steps to address this deficiency. The use of botnets could be used to amplify narratives at home and abroad, but could also be used to specifically target enemy social media messaging, as Fernandez did to counter IS narratives with the CSCC.[104] We must consider botnets just as we do any other weapon in our arsenal; to be used with judicious care in the proper circumstances to defeat the enemy.

THE RISKS

The employment of botnets for message amplification is a significant step for the CAF into grey zone warfare.[105] It marks a departure from the policies enshrined in our current directives.[106] Furthermore, it stands at odds with the arguments put forward by Brigadier-General Jay Janzen, the current director of Strategic Communication for the CAF.[107] Although Janzen advocates for the establishment of networks of military personnel to reinforce messaging, this paper argues that this will remain insufficient in the near term. Without the initial "shock and awe" of virality, the reinforcing fires of

---

[103] Szoldra, "Military Leaders are Starting to freak Out Over Russia's Information Warfare Dominance."

[104] Patrikarakos, *War in 140 Characters,* 240.

[105] Carment & Belo, "War's Future."

[106] Assistant Deputy Minister Public Affairs, *DND/CF Guidelines for the External Use of Social Media*, 4-5.

[107] Janzen, *What if the Pen IS a Sword?*, 21-22.

CAF members will not be enough to win the battle of the narrative on social media.

Beyond simply a change in policy, the establishment of botnets for promotion of messaging can be seen as a Pandora's Box. Although used for promotion purposes, a botnet can easily be reoriented for targeted cyber attacks such as DDOS. How then do we ensure that it does not become employed in such a manner?[108] At this time, there is no clear system in place to control this use, nor is there currently a method for synchronizing with the efforts of the rest of the Government of Canada — a potentially fatal gap. This lack of synchronization could also lead to a breakdown in relationships with allies or in the established protocols that Western governments use to legitimize their own relationships with their citizens, such as open communication.[109]

Addressing concerns related to a whole of government approach to social media is beyond the scope of this paper, but is worth further study. The use of botnets to enhance Government of Canada messaging could play a critical role in combatting harmful adversary messaging, but its use would have to be strictly controlled.[110] Concerns over partisanship and politicization of such a tool, whether restricted to the CAF or not, would need to be addressed.[111] These risks should be analyzed, as we could operationalize a powerful tool in the struggle against grey zone warfare and asymmetric threats.[112]

CONCLUSION

The Western world faces significant danger from adversaries who are capable of

---

[108] Brezo, JDe La Puerta, Santos & Barroso. "C&C Techniques in Botnet Development," 2-3.
[109] Carment & Belo, "War's Future."
[110] Communications Security Establishment, *Cyber Threats to Canada's Democratic Process,* 20.
[111] Herrmann, *'Truth': Why Spock is Such an Unusual Character*, 24.
[112] Carment & Belo, "War's Future."

exploiting social media.[113] These enemies have exploited gaps in Western plurality and trust in communications systems in multiple ways, including through the use of botnets for propaganda purposes. The CAF now finds itself outmatched in the moral plane and effectively unarmed in the social media arena. It must adopt new methods in order to address this, and the most obvious answer is the employment of botnets for its own purposes.

Although this is ethically distasteful, there is nothing inherently illegal about the use of botnets for the promotion of information. Peter Singer, 21st century war and politics specialist and co-author of *Likewar,* acknowledges that promotion may be necessary as "truth won't go viral merely because it's true."[114] There are considerations of the dubious nature of self-promotion, and there is no denying that there would likely be perceptions that such activity is beneath the CAF, but we must recognize that paradigm has shifted. These perceptions must be transcended; the CAF must recognize that the value and truth of messaging is marginal if it can never be heard by the target audience. We no longer live in a world where the overall worth of a message is the crucial element of its value; its ability to reach the multitudes who can share and amplify is what truly matters.[115]

The suggestion that the CAF engage botnets to amplify and promote its message

---

[113] *Ibid.*

[114] Peter Singer, Twitter post, 4 May 2019, 11:04 a.m., accessed 4 May 2019, https://twitter.com/peterwsinger/status/1124691151863394304. Singer is the current strategist for the New America Foundation and a former Senior Fellow at the Brookings Institute where he was director of the Centre for 21st Century Security and Intelligence. He is considered a global expert on 21st century warfare and his work *Likewar* with Brooking was described as "required reading for everyone living in a democracy and all who aspire to."

[115] Kolga, *Stemming the Virus*, 41.

is contentious. It is to be expected that debate over the ethics of using the tool that our adversaries employ would arise. However, the nature of Web 2.0 social media platforms puts them beyond the effective control of most national governments, and to do nothing would leave ourselves vulnerable to the threats of enemies who have demonstrated a prodigious ability to shape the moral plane through social media. If the CAF is unwilling to marshal its forces, to take up botnets as the weapons it needs, then it will effectively surrender the battlespace to the enemy with potentially catastrophic consequences.

Bibliography

Assistant Deputy Minister Public Affairs. *DND/CF Guidelines for the External Use of Social Media.* Ottawa : Department of National Defence, 2011.

Berger, J.M. "How ISIS games Twitter." Last accessed 28 April 2019, https:// www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

Brezo, Felix, Jose Gaviria De La Puerta, Igor Santos & David Barroso. "C&C Techniques in Botnet Development" in *International Joint Conference CISIS 12-ICEUTE Special Sessions.* Seville : CISIS, 2012.

Brooking, Emerson T. & P.W. Singer. "War Goes Viral." Last accessed 27 April 2019, https:// www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/

Carment, David & Dani Belo. "War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare." Last accessed 1 May 2019, https://www.cgai.ca/ wars_future_the_risks_and_rewards_of_grey_zone_conflict_and_hybrid_warfare

Clow, Ryan. "Psychological Operations: The Need to Understand the Psychological Plane of Warfare." *Canadian Military Journal*. 9 (1), 21-29.

Communications Security Establishment. *Cyber Threats to Canada's Democratic Process.* Ottawa : Communications Security Establishment, 2019.

Computational Propaganda Project. "Resource for Understanding Political Bots." Last accessed 5 April 2019, https://comprop.oii.ox.ac.uk/research/public-scholarship/resource-for-understanding-political-bots/

Congress of the United States. *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security.* Washington D.C. : Committee on Foreign Relations United States Senate, 2018.

Department of National Defence. *CFJP 01 Canadian Military Doctrine.* Ottawa : Department of National Defence, 2009.

Gallagher, Erin. "Propaganda Botnets on Social Media." Last accessed 28 April 2019, https:// medium.com/@erin_gallagher/propaganda-botnets-on-social-media-5afd35e94725

Giles, Keir. *Handbook of Russian Information Warfare.* Rome : NATO Defence College, 2016.

Gordon. "Winning the Narrative - An Army Officer's Perspective." Last accessed 1 May 2019, https://www.wavellroom.com/2018/07/05/how-do-you-win-the-narrative/?utm_content=buffer4aa3f&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Herrmann, John. *'Truth': Why Spock is Such an Unusual Character.* Phoenix : Weaponized Narrative Initiative for the Center on the Future of War, 2017.

Janzen, Col Jay. *What if the Pen IS a Sword? Communicating in a Chaotic, Sensational, and Weaponized Information Environment.* Toronto : Canadian Forces College, 2018.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security.* 38:2, 7-40.

Kolga, Marcus. *Stemming the Virus: Understanding and Responding to the Threat of Russian Disinformation.* Toronto : Macdonald-Laurier Institue, 2019.

Mueller, Robert S. *Report on the Investigation Into Russian Interference in the 2016 Presidential Election, Volume I of II.* Washington DC : United States Department of Justice, 2019.

Patrikarakos, David. *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century*. New York : Basic Books, 2017.

Poulsen, Kevin. "Air Force Colonel wants to build a military BotNet." Last accessed 20 April 2019, https://www.wired.com/2008/05/air-force-col-w/

Regester, Virginia. *an Assessment of Botnets as an Offensive Cyber Weapon for the United States.* New York : Utica College, 2015.

Seaboyer, Anthony. *Influence Techniques Using Social Media.* Kingston : Defence Research and Development Canada, 2018.

Singer, P.W. & Emerson T. Brooking. *Likewar: The Weaponization of Social Media.* New York : Houghton Mifflin Harcourt, 2018.

Szoldra, Paul. "Military Leaders are Starting to freak Out Over Russia's Information Warfare Dominance." Last accessed 22 April 2019, https://taskandpurpose.com/russia-information-war

United States Department of Justice. *United States v. Internet Research Agency et al.* Washington D.C. : District Court for the District of Columbia, 2018.

United States Department of Justice. *Affidavit in Support of an Application for a Criminal Complaint for Mariia Butina*. Washington D.C. : District Court for the District of Columbia, 2018.

Watts, Clint. "Clint Watts' Testimony: Inside Russia's Fake News Playbook." Last accessed 30 April 2019,https://www.thedailybeast.com/inside-russias-fake-news-playbook

Zakem, Vera, Megan K. McBride & Kate Hammerberg. *Exploring the Utility of Memes for U.S. Government Influence Campaigns.* Arlington : CNA Analysis & Solutions, 2018.

Zhang, Jinxue, Rui Zhang, Yanchao Zhang & Guanhua Yan. "The Rise of Social Botnets: Attacks and Countermeasures." *IEEE transactions on Dependable and Secure Computing.* 15:6, 1068-1082.

Zhang, Jinxue, Rui Zhang, Yanchao Zhang & Guanhua Yan. "On the Impact of Social Botnets for Spam Distribution and Digital-Influence Manipulation" in *Record of the 2013 IEEE Conference on Communications and Network Security.* Washington DC : IEEE Computer Society, 2013.

Zhang, Xianchao, Shaoping Zhu & Wenxin Liang. "Detecting Spam and Promoting Campaigns in the Twitter Social Network" in *Record of the 2012 IEEE 12th International Conference on Data Mining.* Washington DC : IEEE Computer Society, 2012.