Bot Activity in the 2020 Singaporean Elections: A Social Cybersecurity Analysis*

Joshua Uyheng[1 [0000−0002−1631−6566]], Lynnette Hui Xian Ng[1 [0000−0002−2740−7818]], and Kathleen M. Carley[1 [0000−0002−6356−0238]]

CASOS Center, Institute for Software Research, Carnegie Mellon University, Pittsburgh PA 15213, USA
{juyheng,huixiann,kathleen.carley}@cs.cmu.edu

Abstract. This paper performs a social cybersecurity analysis of the 2020 Singaporean elections. Harnessing a dataset of 240,000 tweets about the elections, we find that 26.99% of participating accounts are bots. Psycholinguistic analysis shows that bots use simpler and more abusive, second-person language; hashtag usage further indicated that bots propagated messages about COVID-19 and voter suppression. Bots were also associated with denser but less echo chamber-like communities. However, despite their distinct narrative and network features, we find that bots generally did not hold significant influence over the online conversation. We discuss implications for online disinformation during the ongoing COVID-19 pandemic, both in the Asia-Pacific and beyond.

Keywords: Social Cybersecurity · Bots · Elections · Singapore · COVID-19.

1 Introduction

Extensive studies in social cybersecurity tackle the large-scale efforts of inauthentic accounts like bots and trolls to sway public opinion on digital platforms [3, 4]. An important area of research concerns the development of computational tools to identify and characterize such information operations [2]. Amidst an ongoing global pandemic, such research efforts become crucial especially during high-profile events like national elections, where coordinated online activities bear potential to undermine democratic practice or exert foreign influence [11, 12]. In this view, a shared concern in the field regards the extent to which information

* This work was supported in part by the Knight Foundation and the Office of Naval Research grants N000141812106 and N000141812108. Additional support was provided by the Center for Computational Analysis of Social and Organizational Systems (CASOS) and the Center for Informed Democracy and Social Cybersecurity (IDeaS). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Knight Foundation, Office of Naval Research or the U.S. government.

operations become successful, how they achieve such success, and whether their dynamics can be understood in a systematic fashion.

Although literature in this area has grown significantly in recent years, much of the evidence base remains concentrated in Western contexts [10]. Online disinformation, however, is a ubiquitous phenomenon across various geopolitical settings; regional differences challenge and refine normative assumptions about the nature and processes of online disinformation [6]. For instance, studies in non-Western societies present unique challenges in a discipline where many tools are often biased toward English and the activities of Euro-American users.

In July of 2020, Singapore held its general election to choose members of its 14th Parliament. Although the incumbent People's Action Party had held overwhelming majority power for decades, this year's campaigns featured rising tides of support for the progressive and youth-oriented Worker's Party. Given pandemic-related disruptions and restrictions, national polls likewise took place at a volatile time. Meanwhile, in the year prior, Singapore had enacted the Protection from Online Falsehoods and Manipulation Act (POFMA), which imposed large penalties for engagement in fake news propagation [7].

Amid pandemic-fueled economic uncertainty, did generational shifts in political sentiment create an environment ripe for online disinformation? Or did stringent legislation secure online discourse from widespread interference? Here, we do not make causal claims about these complex situations. Instead, this paper presents a descriptive analysis of Twitter conversations surrounding the 2020 Singapore elections. Such evidence may provide valuable basis for advancing higher-level inquiry. From a methodological standpoint, we also show how flexible and generalizable tools can be used within a linguistically diverse setting. Our motivation is not to design new methods, but rather to demonstrate how existing models may be integrated to tackle real-world problems [12]. We also present practical insights for worldwide elections more broadly.

2 Data and Methods

2.1 Data Collection

To sample the online conversation about the 2020 Singaporean elections, we employed Twitter's rest API. Data collection was performed on a daily basis using general hashtags related to election discourse (e.g., #GE2020, #sgelections2020) and more specific terms related to prominent parties (e.g., @PAPSingapore, @wpsg) and parliamentary candidates (e.g., @jamuslim). Search terms were updated and validated based on manual searching of ongoing Twitter conversations. Data collection began June 18 - a week before the previous parliament was dissolved for the elections - and concluded July 17 - a week after election day. A total of 240K tweets were collected featuring 42K unique users. Data will be made available through KiltHub on reasonable request[1].

[1] https://kilthub.cmu.edu/authors/Joshua_Uyheng/5971211

2.2 Bot Detection with BotHunter

We used the BotHunter algorithm to identify inauthentic accounts in our dataset. BotHunter is a machine learning algorithm based on a random forest model trained on a large dataset of known bots [2]. Employing a tiered approach, BotHunter utilizes account and network features to generate probabilistic predictions of whether an account is bot-like or not. BotHunter also features comparable predictive performance to existing bot detection algorithms in the literature.

2.3 Psycholinguistic Cues with Netmapper

To characterize bot messages, we relied on psycholinguistic cues. A rich tradition in social psychology associates the use of particular words and expressions with behavioral, cognitive, and emotional states [8], as well as deceptive and persuasive communication [1]. Using the Netmapper software[2], we count the frequency of key lexical categories including abusive terms, absolutist terms, exclusive terms, and positive and negative terms [5]. Netmapper is particularly useful in the Singaporean setting given its multilingual functionality, covering over 40 languages. Harnessing these measures, we specifically sought to distinguish the language employed by bot and human accounts.

2.4 Social Network Analysis with ORA

Finally, we used ORA for social network analysis [5]. ORA[3] is an integrated tool for the analysis of large-scale, complex networks. We represented our Twitter corpus as a complex graph structure which contained multiple types of nodes - agents, tweets, and hashtags - featuring multiple types of edges, including: agent by agent communication through retweets, replies and mentions; agent by tweet relationships based on who send what; agent by hashtag usage networks; and tweet by hashtag connections based on the hashtags contained per tweet. These network structures enable a wide variety of pertinent analysis for social media conversations, including the measurement of user influence and the automatic detection of emergent community structure. For the former, numerous measures of centrality abound for assessing different notions of user importance within a network structure [5]. For the latter, we use the Leiden clustering algorithm, a known improvement over the Louvain clustering algorithm, which boasts mathematical guarantees for non-degenerate groups and faster run-time [9].

3 Results

Our findings reveal significant bot activity on Twitter surrounding the 2020 Singaporean elections. Using our interoperable pipeline of social cybersecurity tools, we further present a nuanced picture of distinct bot behaviors as well as evidence that their influence over the online conversation was relatively low.

[2] http://netanomics.com/netmapper/
[3] http://netanomics.com/ora-pro/

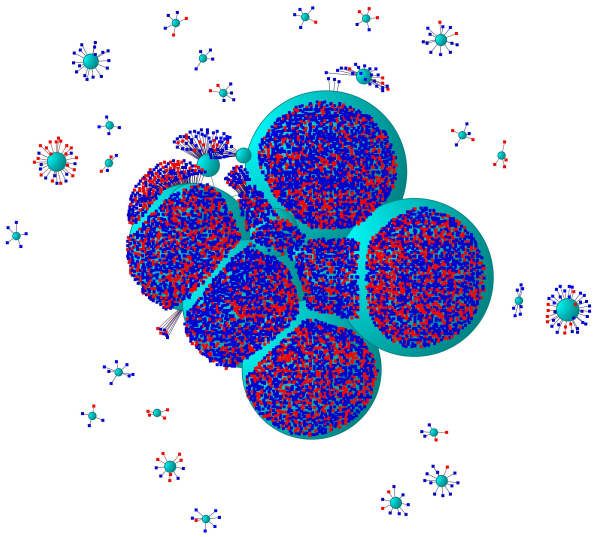

Fig. 1. ORA visualization of Twitter conversation surrounding 2020 Singaporean elections. Accounts are represented as nodes connected to larger meta-nodes based on Leiden clusters. Clustering was obtained on the network with the sum of all retweets, replies, and mentions as edges. Node colors are red if BotHunter probability is greater than 0.8, and blue otherwise. Clusters of size less than 3 dropped from plot.

3.1 Bot Prevalence and Interactions

Figure 1 depicts the network of users in our dataset based on their combined retweets, replies, and mentions. The proportion of red nodes (which represent bots) suggests a significant number of bots participating in the Twitter conversation. They also appear relatively ubiquitous given their presence in virtually all Leiden clusters. Figure 2 quantifies these observations, showing that the distribution of BotHunter probabilities is skewed to the left, with a mean value of 0.62. At a 0.8 probability threshold for bot-likeness, 26.99% of unique users in our dataset may be classified as bots.

Figure 2 further suggests that bots did not only constitute a large proportion of the users participating in the conversation; more bot-like accounts also produced more tweets on average. We observe a clear upward trend, with the most bot-like accounts producing about twice as many tweets as the most human-like accounts. But bots generally performed fewer interactions than humans, despite producing more tweets on average. This suggests bots produced many original tweets not directed at others. Furthermore, both bots and humans talk to humans more, as 56.09% of all interactions took place between humans, while 6.40% of all interactions came from bots directed at humans. But 32.66% of all communication by humans was also directed at bots. Whether knowingly or not, humans frequently communicated with bots.

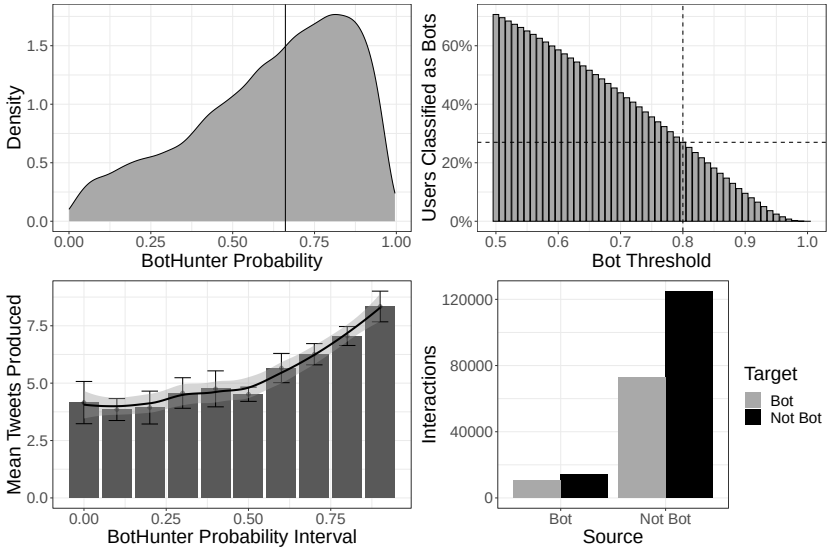

Fig. 2. Bot prevalence and behavior. **Top-Left:** Density plot of unique users' bot probabilities using BotHunter. Vertical line indicates mean value of bot probabilities at 0.62. **Top-Right:** Bar plot indicating percentage of bots at different BotHunter probability thresholds. At a 0.8 threshold (vertical line), 26.99% of unique users are classified as bots (horizontal line). **Bottom-Left:** Mean number of tweets produced by users at different intervals of BotHunter probabilities in 0.1 increments. Error bars represent 95% confidence intervals with fitted loess trend. **Bottom-Right:** Number of interactions between bots and humans based on a 0.8 probability threshold.

3.2 Bot Aggression and Electoral Distrust

Besides interaction patterns, the language used by bots also featured notable differences from humans. Figure 3 shows the coefficients of a regression model relating BotHunter probability scores to users' psycholinguistic cues. All variance inflation factors ranged from 1.02 to 1.28, indicating no multicollinearity problems. Most notably, we saw that bots used much simpler language than humans as denoted by the Reading Difficulty score. Human accounts were also significantly more likely to refer explicitly to identity terms related to gender or politics, as well as positive-sentiment terms. In contrast, we found that bots were more likely to use abusive terms, absolutist terms, exclusive terms, second-person pronouns, and identity terms related to family (e.g., father, mother). This suggests that bots were engaged in insulting behavior directed toward the people they interacted with. Finally, no significant differences were seen between bots and humans relative to the use of negative-sentiment terms, first-person or third-person pronouns, and identities related to race and religion.

Hashtag usage features three broad patterns. Figure 4 plots all hashtags used by bots and humans, ranked according to their average usage by both account types. The first pattern is suggested by the diagonal line. Many high-ranking

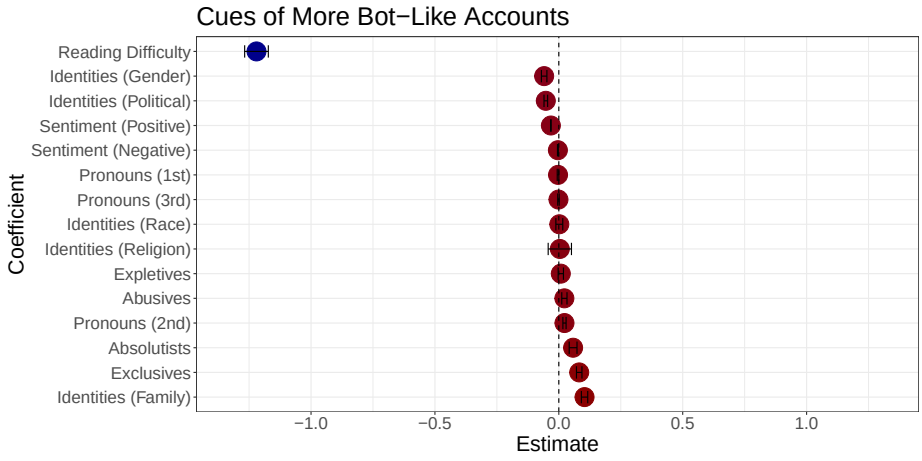

Fig. 3. Psycholinguistic cues which distinguish bots and humans. Points represent coefficient estimates in a multiple regression model predicting bot probability based on lexical features. Error bars represent 95% confidence intervals. Intersection of confidence intervals with the origin (broken line) indicates non-significant effects.

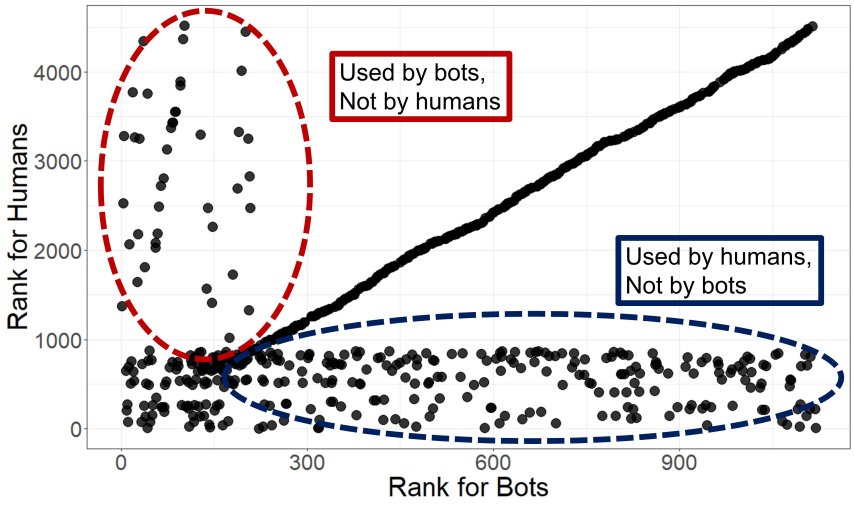

Fig. 4. Scatterplot of hashtag ranking based on mean usage by bots and humans. Higher values indicate lower ranks. Hashtags on the bottom-right are ranked higher for humans than bots; hashtags on the top-left are ranked higher for bots than by humans.

hashtags for humans were also high-ranking for bots. Conversely, many low-ranking hashtags for humans were also low-ranking for bots. A second pattern concerns hashtags in the blue cluster, which were used frequently by humans

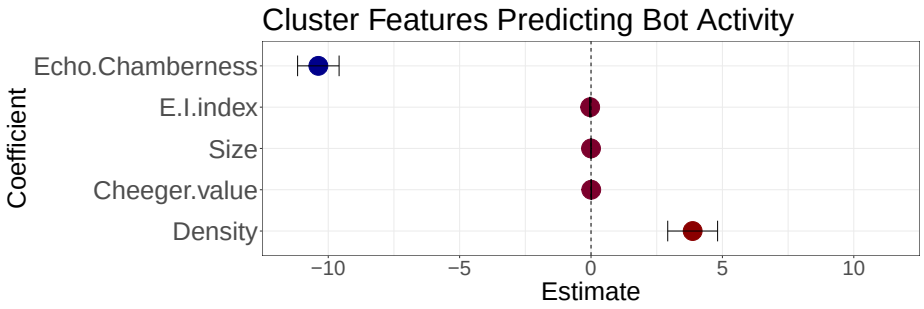

Fig. 5. Structural features distinguishing Leiden clusters with high or low bot activity. Points show coefficient estimates in a multiple regression model of average bot probability based on cluster structure. Error bars represent 95% confidence intervals.

and not by bots. Interestingly, this category largely included anti-incumbent and pro-opposition hashtags, such as #youdeservebetter,#VoteThemOut, #PartyAgainstPeople (a play on the incumbent People's Action Party), #voteWP (the opposition Workers Party), and #WPJamusLimFanClub (a popular opposition candidate). This indicated sizeable organic support for the opposition party, expressed in distinct ways relative to bots. More general references to the election were also found, such as #SingaporeGeneralElection2020, #SingapuraMemilih ('Singapore Choose' in Malay), and #VoteWisely. Hence, we saw that humans generally produced more mainstream messaging than bots.

Meanwhile, a third pattern is denoted by the red cluster. We observe several hashtags which had high rank for bots, but low rank for humans. The top 50 hashtags higher in rank for bots than for humans included: (a) the opposition Worker's Party (e.g., #WORKERSPARTY2NDWIN), (b) references to COVID-19 (e.g., #WashYourHands), (c) talk about electoral distrust (e.g., #votersuppression), and (d) spam content (e.g., #XboxSeriesX). These broadly suggest that bots engaged in distinct message strategies. Bots were variously concerned with discussing opposition to the long-standing incumbent, highlighting the pandemic and its possible impact on the elections, as well as possibly using electoral hashtags for opportunistic marketing, as seen in prior research [12].

3.3 Bot Cluster Density and Community Interference

Bots operate not just through the messages they send, but also through manipulating social network structure based on artificial patterns of interaction with other users. Based on the results of Leiden clustering, we therefore asked: What structural features distinguish clusters with higher bot activity?

Regression analysis indicated that clusters featuring high bot involvement were denser, indicating higher levels of internal communication. This suggests that bot activity potentially takes place in relatively coordinated groups. On the other hand, clusters with primarily human activity were more echo chamber-like. Hence, bot involvements tended to break down echo chambers, thereby

Table 1. Most influential accounts in 2020 Singaporean elections. A '+' indicates verified accounts; a '*' indicates news accounts.

Rank	Super Spreaders	Super Friends	Other Influencers
1	wpsg^{+}	eisen	Reuters$^{+,*}$
2	ChannelNewsAsia$^{+,*}$	historyogi	Cristiano^{+}
3	plspreeti^{+}	tanhuiyi	leehsienlong^{+}
4	jamuslim^{+}	sgelection	wpsg^{+}
5	tzehern_	kixes^{+}	narendramodi^{+}
6	historyogi	guanyinmiao	historyogi
7	eisen	mdzulkar9	jamuslim^{+}
8	RaeesaKhanwpsg^{+}	plspreeti^{+}	nytimes$^{+,*}$
9	mediumshawn	mediumshawn	sgelection
10	MothershipSG^{+}	BenChiaCars	fat__thin

bridging different groups. Cluster size did not relate to levels of local bot activity; neither did the E/I index or the Cheeger score. All variance inflation factors in this regression model ranged from 1.18 to 3.44, indicating no multicollinearity problems.

3.4 Bot Failure to Amass Network Influence

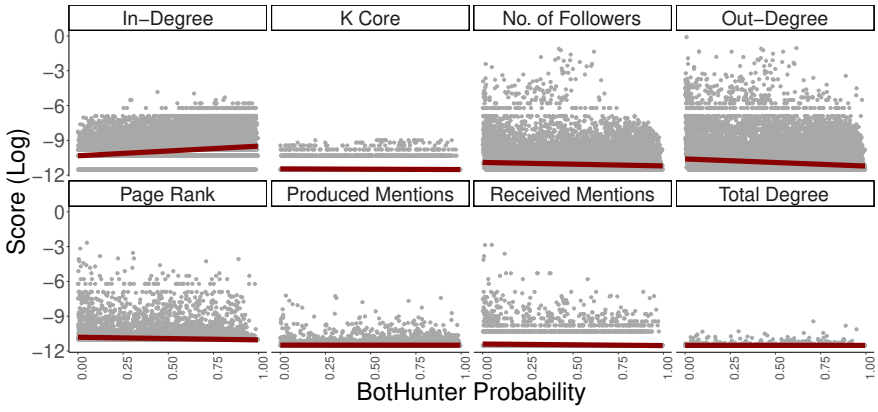

Fig. 6. Scatter plots of influence scores (log) versus bot probabilities. Blue lines denote fitted linear regression models.

Finally, we consider the level of influence bots had relative to other users in the dataset. ORA summarizes super spreaders, super friends, and other influencers in the online conversation. *Super spreaders* generate highly shared content, measured by average ranking on out-degree centrality (many share their

content), page rank centrality (they interact with other influential accounts), and large k-core membership (belong to large cluster). *Super friends* engage in extensive two-way communication, again identified by highest average ranking on total degree centrality (total interactions) and large k-core membership. *Other influencers* are influential in other ways, by having high numbers of followers, or high levels of mentioning and being mentioned.

Table 1 provides the top 10 accounts for each of the three categories. Generally, it seems that the most influential accounts are verified accounts and news accounts. The opposition Workers Party, in particular, dominates the list by having their party account and individual candidates feature as super spreaders and other influencers. Incumbent Prime Minister Lee Hsien Long only appears among the top 10 other influencers. Bot accounts did not occupy dominant positions in these influencer lists either. Figure 6 visualizes the full distribution of influence metrics used by ORA relative to bot probabilities. In all measures but one, bots were not more influential. Most bots did not belong to larger k cores, did not have more followers, did not have more viral content, did not interact with more influential accounts, and neither received nor produced the most mentions and total interactions. However, bots tend to have higher in-degree, indicating that they produced more retweets, replies, and mentions in attempts to gain influence, but not securing it meaningfully in the larger conversation.

4 Conclusions and Future Work

We reflect on four implications of our quantitative portrait of Twitter disinformation during the 2020 Singaporean elections. First, we highlight disruptive bot messaging related to COVID-19 and voter suppression. Notwithstanding genuine concerns the pandemic poses for equitable elections, researchers may examine how future information operations use these concerns to undermine democratic practice. Second, we consider the effects of POFMA [7]. Although we did not explicitly find fake news sharing, we detected bot signals comparable with other Asia-Pacific countries without strict legislation [10]. This raises questions about disinformation's flexibility - exceeding falsehoods to include hostility and discord - and effective ways of curbing it without curtailing free speech. Third, we observe that the opposition held more online influence than the incumbent, but the latter still won parliamentary majority. This is consistent across recent elections in the Philippines, Indonesia, and Taiwan [11], suggesting that regional links between online popularity and electoral success are not straightforward. Fourth, we affirm the importance of designing interoperable pipelines for social cybersecurity [12]. We show how the problem-oriented integration of existing tools can quantify unique narrative and network features of disinformation actors [3, 4], and provide (negative) evidence of their influence over the broader conversation.

Several limitations nuance our conclusions from this work. Sampling Twitter data remains limited by API generalizability issues, suggesting nuance in extrapolating findings to wider contexts. We also reiterate our primarily empirical, rather than methodological, goals in this research. To improve these computa-

tions, algorithmic developments may more explicitly consider local patterns of language and social media use. Multi-platform studies would also aid more holistic inquiry into online electoral discourse given that Twitter may not play the same role here as in the West.

References

1. Addawood, A., Badawy, A., Lerman, K., Ferrara, E.: Linguistic cues to deception: Identifying political trolls on social media. In: Proceedings of the International AAAI Conference on Web and Social Media. vol. 13, pp. 15–25 (2019)
2. Beskow, D.M., Carley, K.M.: Bot conversations are different: Leveraging network metrics for bot detection in twitter. In: 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). pp. 825–832. IEEE (2018)
3. Beskow, D.M., Carley, K.M.: Social cybersecurity: An emerging national security requirement. Military Review **99**(2), 117 (2019)
4. Carley, K.M., Cervone, G., Agarwal, N., Liu, H.: Social cyber-security. In: International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation. pp. 389–394. Springer (2018)
5. Carley, L.R., Reminga, J., Carley, K.M.: ORA & NetMapper. In: International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation. Springer (2018)
6. Humprecht, E., Esser, F., Van Aelst, P.: Resilience to online disinformation: A framework for cross-national comparative research. The International Journal of Press/Politics p. 1940161219900126 (2020)
7. Tan, N.: Electoral management of digital campaigns and disinformation in East and Southeast Asia. Election Law Journal: Rules, Politics, and Policy (2020)
8. Tausczik, Y.R., Pennebaker, J.W.: The psychological meaning of words: LIWC and computerized text analysis methods. Journal of Language and Social Psychology **29**(1), 24–54 (2010)
9. Traag, V.A., Waltman, L., van Eck, N.J.: From Louvain to Leiden: Guaranteeing well-connected communities. Scientific Reports **9**(1), 1–12 (2019)
10. Uyheng, J., Carley, K.M.: Characterizing bot networks on Twitter: An empirical analysis of contentious issues in the Asia-Pacific. In: International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation. pp. 153–162. Springer (2019)
11. Uyheng, J., Carley, K.M.: Bot impacts on public sentiment and community structures: Comparative analysis of three elections in the Asia-Pacific. In: International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation. Springer (2020)
12. Uyheng, J., Magelinski, T., Villa-Cox, R., Sowa, C., Carley, K.M.: Interoperable pipelines for social cyber-security: Assessing Twitter information operations during NATO Trident Juncture 2018. Computational and Mathematical Organization Theory pp. 1–19 (2019)