Artificial Humanity: Countering the Threat of Bot Networks on Social Media

Yudhanjaya Wijeratne, Sanjana Hattotuwa, Raymond Serrato
CPRsouth
Maputo, Sep 2018

This work was carried out with the aid of a grant from the International Development Research Centre, Canada and the Department for International Development UK.
Social media is a digital agora.
Fill this agora with enough agents, and you eventually control the conversation.
How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument

GARY KING (a1), JENNIFER PAN (a2) and MARGARET E. ROBERTS (a3)

https://doi.org/10.1017/S0003055417000144 Published online: 27 July 2017

Abstract

The Chinese government has long been suspected of hiring as many as 2 million people to surreptitiously insert huge numbers of pseudonymous and other deceptive writings into the stream of real social media posts, as if they were the genuine opinions of ordinary people. Many academics, and most journalists and activists, claim that these so-called 50c party posts vociferously argue for the government's side in political and policy debates. As we show, this is also true of most posts openly accused on social media of being 50c. Yet almost no systematic empirical evidence exists for this claim or, more importantly, for the Chinese regime's strategic objective in pursuing this activity. In the first large-scale empirical analysis of this operation, we show how to identify the secretive authors of these posts, the posts written by them, and their content. We estimate that the government fabricates and posts about 448 million social media comments a year. In contrast to prior claims, we show that the Chinese regime's strategy is to avoid arguing with skeptics of the party and the government, and to not even discuss controversial issues. We show that the goal of this massive secretive operation is instead to distract the public and change the subject, as most of these posts involve cheerleading for China, the revolutionary history of the Communist Party, or other symbols of the regime. We discuss how these results fit with what is known about the Chinese censorship program and suggest how they may change our broader theoretical understanding of “common knowledge” and information control in authoritarian regimes.
However, it is now easier to do this at scale than ever before – one can simply write software-operated accounts – aka “bots” - to mimic humans.

These bots can operate in coordinated networks, masquerade as humans, seize control of this public space and create the illusion of overwhelming social proof behind any cause the operators chose to champion.
Our analysis of block lists and over 214,000 tweets shows the existence of at least 4,603 such accounts targeting Sri Lankans on Twitter.

Analysis of a 25% sample shows that these accounts:
   a) mimic names from major ethnicities in the country to give the illusion of representativity
   b) follow the same set of prominent influencers and political activists, especially people who share relatively large amounts of web links
South-east Asia sprouts fake followers for prominent Twitter users

State-run agencies under suspicion as thousands of new accounts emerge
Mexico’s Troll Bots Are Threatening the Lives of Activists

How an army of Twitter trolls is invading Mexico’s democratic process.

How Twitter Bots Help Fuel Political Feuds

 Automated social media accounts can create “misinformation networks” that spread falsehoods and fan the flames of partisan disagreement

By Chris Baraniuk on March 27, 2018

The Twitter Bot That Sounds Just Like Me

Hackers can use artificial intelligence to mimic their targets’ tweets—and entice them to click on malicious links.

KAVEH WADDELL  AUG 16, 2016
What was once a problem for the West is now becoming a problem for democracy in the Global South.

Operators of the social networks that host these bots have been shown to be often unaware, incapable or unwilling to deal with them.
How do we detect these bots?

- Requires both qualitative analysis – to identify pockets of suspicious activity – and big-data oriented tools and infrastructure.

- Significant investments in technology and personnel required even for rudimentary analysis.
Once detected, what then?
It is impossible to combat this with sophisticated detection alone. This requires a complex interaction of technical, social and legal frameworks.

1) Invest in monitoring operations, ideally as a collaboration between government ICT bodies and journalists, that can utilize computer-aided analysis and human interpretation to regularly detect social bot networks, especially with regards to the addition of artificial social weight to information and disruption of public discourse.

2) **We need to discourage the impersonation of digital identities.** Because this interacts with issues of privacy and self-identification on the internet, this issue should be approached with caution and with public and civic consultation.

3) Governments need to create legal mechanisms for punitive action against operators of social bots – after the establishment of malicious intent, which will require local research to establish for each country.

Solving this is a process that begins here.