A Tutorial on Bot-Like Behavior on Twitter

Instructors: David A. Broniatowski, Lulwah AlKulaib, SiHua Qi

This tutorial will introduce the audience to the basics of Twitter account analysis and how to differentiate standard users from automated accounts, with a specific focus on malicious accounts (bots, trolls, and cyborgs). Topics will include statistical features that are associated with bot accounts, bot-like behavior, different types of bots, and an overview of available tools that measure Twitter's accounts bot-likelihood. Attendees will learn the behavior exhibit by different bot account types, including qualitative analysis of different bot-generated content. In addition, we will provide an overview of existing and novel bot detection methods. Examples of each of these will be provided in the context of vaccination.

c. Agenda:

Section I: Bots, Trolls, and Cyborgs: A Taxonomy of Online Actors (50 minutes)

- What are bots? Malicious and non-malicious actors
- Legitimate Twitter account overview
- Why is it important to identify bots?
- How to identify bots?
- What are the different bot types?
- Generating lists of bots: honeypots

<break>

Section II: Bot-Like Behaviors (50 minutes)

- Bot-like behaviors
- Bot machine-learning features
- Anatomy of a bot
- Example of Python script using Twitter API
- Example of bot-o-meter analysis

<break>

Section III: Case Studies (60 minutes)

- Findings on bot and troll activity in vaccination
- Qualitative analysis of troll-generated content
- Statistical features associated with bot like behaviors
- Strategies used by sophisticated bots
- Preliminary findings on bot classification

Laptops are not required, but Jupyter code for Botometer will be available.

Affiliations: David A. Broniatowski, Lulwah AlKulaib, SiHua Qi, The George Washington University, Amelia Jamison, University of Maryland