Q&A: Botnets and information warfare

December 22 2022, by Ruth Almodal

Credit: Pixabay/CC0 Public Domain

In 2017, City, University of London research by Dr. Marco Bastos was featured in exclusive story by BuzzFeed. The article, by City Journalism alumnus James Ball, lifted the lid on a network of malicious bots that sought to undermine the UK Brexit referendum vote.

The story spread like wildfire, becoming national and international news. With half a decade having passed since the story broke, we spoke to Dr.

Bastos to see how the world of bots and misinformation looks five years on. And, of course, we had to ask about a certain person's recent purchase of Twitter, too…

How did you first discover the Twitterbots and what was your approach to researching it?

It was actually accidental. Shortly after the European Union Referendum Act 2015 passed by Parliament, I set up a data collection pipeline that would identify and monitor British users talking about Brexit on Twitter.

I called this cohort "BTMAU" for British Twitter Monthly Active Users and I kept track of them over the years. In 2017, I noticed that a significant portion of this population disappeared from the platform, and upon probing the data it became clear it was a botnet removed by Twitter themselves.

Using your research, Damian Collins MP wrote to Twitter and later Facebook about possible interference. He also took his inquiry to the US. What policy changes regarding the areas covered in this investigation have we seen in the years since, politically or on the platforms themselves?

There have been important (if slow) developments in the years that followed the study, including design changes implemented by the platforms, but also policy changes implemented by regulatory frameworks. The latter is yet to prove it can make a dent on this problem.

Much of the Digital Service Act (DSA), a body of regulations set to

become law in the next 12 months, is dedicated to illegal content, transparent advertising, and, of course, disinformation. The policy changes have indeed been slow, as they usually are, but the expectation is that the DSA will dramatically change the framework where social platforms operate.

What role have botnets played in the current war between Ukraine and Russia?

Attrition warfare usually follows or precedes information warfare, and this war is no exception. In fact, the data I have looked at seems to indicate that Euromaidan (the wave of demonstrations and civil unrest in Ukraine, which began on 21 November 2013) was the ground zero for the Russian influence operation that was later upscaled to interfere with Western elections.

More generally, how have botnets contributed to tensions between the UK, Russia and the US in the years following your study?

Botnets are still very much in operation and play a key role in influence operations, including the recent attacks on high-profile politicians in the U.K. and the U.S.

This year, Twitter announced they identified and removed 22 accounts that posted 255,604 tweets in English with the hashtag #Ukraine with the presumptive country of origin being China and the U.S..

They further removed 1,780 accounts that posted 8,920 tweets in Spanish with self-reported user location in Guatemala, but the presumptive countries of origin was Russia and Ukraine.

Twitter, however, has since laid off several employees who worked on the identification and removal of misinformation, particularly Foreign Information Manipulation and Interference (FIMI).

That brings us onto Elon Musk and his recent high-profile purchase of Twitter. Do you expect that the situation may improve or worsen regarding outside influences on politics?

It's early days to make a call, but there has been a considerable migration to Mastodon. I believe decentralized, federation-based social media platforms are likely to somewhat slow down the elapsed effects of social platforms on politics. This is due to several platform affordances, including a more nuanced combination of public and private communication that can be leveraged to minimize the megaphone effect typical of Twitter campaigning.

What other agendas have we seen these bots being used for? Is it possible they could be used for good?

Bots can absolutely be used for good and much of what makes Twitter interesting is that it's a platform that embraces automation. Indeed, several prominent Twitter accounts are bots, including those of mainstream news outlets that relay breaking news, but also government organizations offering early warning systems for earthquakes and tsunamis. The problem of course is when bots are used to impersonate a third party as sock-puppet accounts, a problem that is further compounded by coordinated inauthentic behavior.

What steps can people take to avoid being influenced by possible bot behavior?

I assume you mean malicious activity by bots impersonating somebody, in which case people could report these accounts. There are some manuals out there detailing typical bot-like features, but these should be taken with a grain of salt. Top of the list include accounts with no profile picture, generic mini bio, username with several numbers or incoherent combination of numbers and letters. Other important markers are account creation date, ratio of followers to followees, and number of messages posted versus number of retweets.

Provided by City University London