# Bots and Social Media

## Interviewee: Yudhanjaya Wijeratne

Featured as a *Forbes* profile: Wijeratne has been nominated for the Nebula award for Messenger, a book he co-authored, and struck a five-book deal with HarperCollins, including a novel written using code and AI tools. His 2017 debut novel, Numbercaste, was optioned for film. Today he wears multiple hats including as a data scientist working in public policy at Sri Lankan think tank LIRNEasia and a futurist working with the UNDP. Wijeratne is a high school dropout who worked his way up in retail and along the way taught himself writing and programming.

Additional information originates on the Goethe Institute website:

He co-founded Watchdog, a fact-checking organization, where he spends much of his time digging into misinformation. He built and operates OSUN, a set of literary experiments using OpenAI technology to test a human+AI collaboration in art.

# Bots: Defined

As defined in an article featured on *Cloudflare*, A bot is a software application that is programmed to do certain tasks. Bots are automated, which means they run according to their instructions without a human user needing to manually start them up every time. Bots often imitate or replace a human user's behavior. Typically they do repetitive tasks, and they can do them much faster than human users could.

Bots usually operate over a network; more than half of Internet traffic is bots scanning content, interacting with webpages, chatting with users, or looking for attack targets. Some bots are useful, such as search engine bots that index content for search or customer service bots that help users. Other bots are "bad" and are programmed to break into user accounts, scan the web for contact information for sending spam, or perform other malicious activities. If it's connected to the Internet, a bot will have an associated IP address.

Bots can be:

- Chatbots: Bots that simulate human conversation by responding to certain phrases with programmed responses
- Web crawlers (Googlebots): Bots that scan content on webpages all over the Internet
- Social bots: Bots that operate on social media platforms

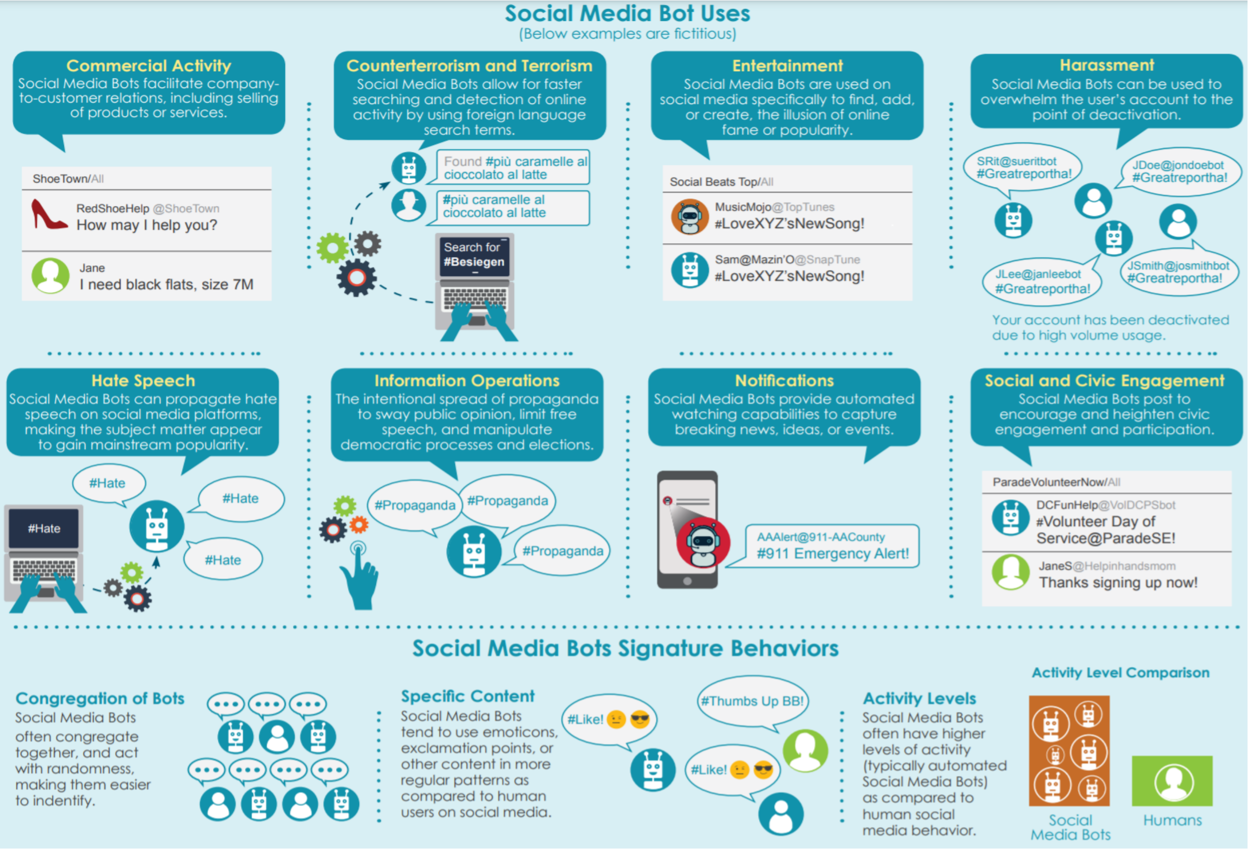
- Malicious bots: Bots that scrape content, spread spam content, or carry out credential stuffing attacks

# Social Media Bots

Sourced from a *Meltwater* article:  The US Government's Office of Cyber and Infrastructure Analysis gives its definition of social media bots as: "Programs that vary in size depending on their function, capability, and design; and can be used on social media platforms to do various useful and malicious tasks while simulating human behaviour. These programs use artificial intelligence, big data analytics, and other programs or databases to imitate legitimate users posting content."

Imperva, a leading cybersecurity company, gives a more succinct and balanced definition: "An internet bot is a software application that runs automated tasks over the internet. Tasks run by automated technology are typically simple and performed at a much higher rate compared to human Internet activity."

Darius Kazemi, a computer programmer and self-proclaimed 'internet artist' who studies the nature and behaviour of these robots, distils the bot definition even further: "A computer that attempts to talk to [people] through technology that was designed for humans to talk to humans." The mighty *New York Times* has its own characterisation: "Those little automatic programs that talk to us in the digital dimension as if they were human."



Social Media Bot Uses

(Below examples are fictitious)

**Commercial Activity**
Social Media Bots facilitate company-to-customer relations, including selling of products or services.

**Counterterrorism and Terrorism**
Social Media Bots allow for faster searching and detection of online activity by using foreign language search terms.

**Entertainment**
Social Media Bots are used on social media specifically to find, add, or create, the illusion of online fame or popularity.

**Harassment**
Social Media Bots can be used to overwhelm the user's account to the point of deactivation.

**Hate Speech**
Social Media Bots can propagate hate speech on social media platforms, making the subject matter appear to gain mainstream popularity.

**Information Operations**
The intentional spread of propaganda to sway public opinion, limit free speech, and manipulate democratic processes and elections.

**Notifications**
Social Media Bots provide automated watching capabilities to capture breaking news, ideas, or events.

**Social and Civic Engagement**
Social Media Bots post to encourage and heighten civic engagement and participation.

Social Media Bots Signature Behaviors

**Congregation of Bots**
Social Media Bots often congregate together, and act with randomness, making them easier to indentify.

**Specific Content**
Social Media Bots tend to use emoticons, exclamation points, or other content in more regular patterns as compared to human users on social media.

**Activity Levels**
Social Media Bots often have higher levels of activity (typically automated Social Media Bots) as compared to human social media behavior.

(Image Source)

# Bots and Social Media

## General Negative Aspects of Social Media Bots

According to *memberpress*: However, bots can harm your social media presence and even your business (not to mention invite malware on your computer!). In the general online presence, a bad bot can do major damage by gathering passwords, logging keystrokes, and even gathering financial information.

It's also been shown that bots can influence trending topics on social media platforms, effectively persuading the opinions of real human users.

Bots can like, follow, and comment on other users' social media platforms, which may seem like a handy feature. But because they aren't human, bots don't understand human context.

They may like, follow, or retweet a hashtag they've been programmed to follow that may not necessarily reflect your brand's ideals or your personal values.

They may also follow accounts that aren't necessarily your target audience or customer avatar. This can cause a disconnect with your followers, some of whom you've worked hard to gain.

And there's one more thing to be especially wary of—bots who create fake accounts or steal people's online identities to promote spam or are part of the "buy X amount of followers" packages shady-businesses offer.

The followers on those accounts are bots and merely serve to inflate the follower count. It's a quantity-over-quality situation where you spend money to get followers but not one of those thousands of followers ever purchases your product.

As featured on *Forbes:*

## Massive Havoc Wreaked By Bots

Research shows that social media channels like Twitter and Facebook are regularly targeted by bad actors to deploy automated bots. Carnegie Mellon estimates that bots are involved in up to 20% of the conversations on social media, especially pertaining to elections and other political issues.

The trend became especially apparent during the June 2016 Brexit vote when, as reported by TechCrunch, "Russian accounts posted almost 45,000 messages pertaining to the EU referendum in the 48 hours around the vote." Of these reported posts, most were bot-driven, and of those, most were in favor of "leave" rather than "remain," the impact of which was further magnified when bot-generated posts were liked and shared by other bots and by human users.

Around the same time, as the 2016 U.S. presidential election campaigns were heating up, the mainstream social media channels were barraged with Russian-operated bot-generated posts in favor of Donald Trump. While Twitter, Facebook and YouTube have started to identity and deactivate false accounts and fake bot postings, bad bots still have a tremendous influence on public opinion.

## Human Life Is Now At Stake

The impact of this malicious trend is not limited to the political arena. Research from the Center for Informed Democracy & Social Cybersecurity at Carnegie Mellon University suggests that “bots may account for between 45 and 60% of Twitter accounts discussing Covid-19.” Many of these accounts spread disinformation and conspiracy theories and sow dissent against state and local orders to wear face masks. Similarly, Brown University found that 25% of climate denial tweets are posted by bots.

It is unsettling to observe the degree to which the national conversation is influenced by automation controlled by actors who do not have our best interests at heart, and it is equally unsettling to see how susceptible we are to being influenced by such forces.

## Tackling The Challenge

The evidence is clear: Bad bot operators have poisoned public debate, derailed civility, and risked human life and well-being.

The time has come to get rid of bad actors. It can be done, but first, there are at least two distinct problems to surmount:

### 1. A Business Model That Disincentivizes The Removal Of Fake Accounts

Social media channels have very little business incentive to eliminate fake accounts. Their entire advertising model rides on their monthly average user counts, especially when these fake accounts generate engagement via likes, click-throughs and retweets that impact the algorithm of popular content shown to users. It wasn't until damaging PR arose from the discovery of Russian-controlled bot influence in the 2016 U.S. election that the social media giants even began to address the problem. And it's not enough. Business models and the regulatory landscape will have to change before bots in social media can be completely eliminated.

The lure of disrupting democratic societies is great, and some actors will go to great lengths to influence hearts and minds. They have the means and tools to infiltrate social media in ever more sophisticated ways. Fortunately, artificial intelligence is helping social media sites track down fake accounts that spew disinformation and sway public opinion. Some of these tools are also available to consumers for Twitter usage, such as NortonLifeLock's BotSight and Bot Sentinel, among others.

AI bot-tracking tools analyze characteristics such as:

- Unusual posting patterns (e.g., a human account isn't likely to create 100 posts in 60 minutes or post for 24 hours straight).
- Discrepancies regarding posts and profile of the person making the posts (e.g., a post written in English with a profile written in another language).

• Hashtags or posts that serve as political triggers and act irregularly (e.g., the same post and hashtags appear at the same instant on thousands of social media accounts).

These are just a few of the many telltale signs of bot behavior. But these behaviors all happen retrospectively — after the bogus account has been created and is generating analyzable activity.

Social media sites must take control and deny access to bots before they darken the doorstep. Not all bots are bad, but those that are simply must not be allowed in the door. Blocking malicious bots before they cross the threshold of social media sites is not too hard. A zero-trust philosophy to online traffic combined with methods to render attacks financially unviable for their operators is not only feasible, but has been proven to be highly effective, based on what my company has seen with clients.

As Americans become more aware of the gravity of the threat of bot-driven disinformation and division, it is my hope that business, government and citizens will unite to wrest online control of the national conversation from malicious actors. The very nature of our democracy and society is at stake.

## Top Social Media Bots

Sourced from *discover.bot*: In 2020, we have seen the rise of social media bots and we expect them to continue to thrive as more businesses move their marketing efforts to the digital space. Based on their effectiveness and safety for users, these are among the year’s best:

- **Nitreo**

This bot allows you to grow your social following by adding niche-specific hashtags and accounts that are similar to yours. According to its website, Nitreo uses SHA-3 cryptographic encryption with Advanced Encryption Standard, which enforces security to your account credentials and keeps your performance results real and accurate.

- **Ingramer**

After taking a break to adapt to new Instagram guidelines, Ingramer promises an effective interaction automation feature and additional functions, like story viewer, post automation, DM manager, and hashtag generator, that can help new businesses to get their profiles together and to steadily grow.

- **Instamber**

Instamber is one of the most affordable options that includes services on platforms like Instagram, TikTok, and Twitter to improve your marketing efforts. This app identifies your usage patterns and activities connected to your IP to create low-risk interactions.

Currently, we have seen how top bots in social media can be used for beneficial aspects in business growth and development. However, it's important to know their various uses and to identify certain activities on social media that could warn of the presence of a malicious social bot.

# Additional Reading

- Instagram Bots: The Pros, The Cons and The Ugly (Apr 2021)
- The Future Is Now - 37 Fascinating Chatbot Statistics
- View of Social bots distort the 2016 US Presidential election online discussion

- Demystifying Social Bots: On the Intelligence of Automated Social Media Actors - Dennis Assenmacher, Lena Clever, Lena Frischlich, Thorsten Quandt, Heike Trautmann, Christian Grimme, 2020