Social Media Bots programs are common and adaptable to various social media platforms across multiple venues and areas of interest. Social Media Bot usage continues to increase on various social media platforms within the United States. As Social Media Bots increase in usage and utility, malicious behavior via Social Media Bots is also likely to increase. Recent elections in 2016 and 2017, in the United States, United Kingdom, France, and Germany, have drawn a spotlight on the nefarious activity of Social Media Bots.

OCIA defines 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 behavior. These programs use artificial intelligence, big data analytics, and other programs or databases to imitate legitimate users posting content.

**Automated Social Media Bots**
Allow the user to establish a set of parameters using programming language within an application or program (e.g., retweet a specific hashtag every time it is posted, but not when the bot itself retweets it), which the Social Media Bot then executes without human interaction.

**Semi-automated Social Media Bots**
Allow a user to program a set of parameters, but may have or require additional user interaction or a greater degree of management. These types of Social Media Bots are typically face accounts with fake personalities and are run at least partially by humans or click farms, rather than being programmed language.

**Common Attack Methods of Social Media Bots**
- **Click Farming or Like Farming** inflate fame or popularity on a website through liking or reposting of content via Click Farms, which provide fake user accounts (typically semi-automated Social Media Bots) and management of the Social Media Bots (e.g., bot herder) for purchase.
- **Hashtag Highjacking** use hashtags to focus an attack (e.g., spam, malicious links) on a specific audience using the same hashtag.
- **Retweet Storm** use a parent Social Media Bot account, or many Social Media Bots, to initiate an attack by reposting something, which an associated group of Social Media Bots (aka botnet) instantly reposts.
- **Sleeper Bots** remain dormant for long periods of time, wake up to launch their attack of thousands of posts or retweets in a short period of time (perhaps as a Retweet Storm, or spam attack), then return to a dormant state.
- **Trend Jacking and Watering Hole Attack** use top trending topics to focus an intended audience for targeting purposes.

**Social Media Bots Signature Behaviors**

- **Hate Speech**
Social Media Bots can propagate hate speech on social media platforms, making the subject matter appear as compared to human users on social media.

- **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 Media Bots Overviews**
To indentify.

**Social Media Bots Uses**
(Below examples are fictitious)

**Commercial Activity**
Social Media Bots facilitate company-to-customer communications, 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 fans of popularity.

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

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

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

**Conclusion**
Social Media Bots are becoming more prevalent and better at mimicking human behavior on social media platforms. As of 2017, technology companies are seeking investments and further incorporation of Social Media Bots into social media services and platforms, expanding “future digital communication” to provide a myriad of services as automated assistants. As Social Media Bots gain a greater foothold in social media and daily life, the potential uses, for good and malicious purposes, are ever expanding.