**Name:** Ronit Singh **CDAD-UH 1037** **Date:** 21 November, 2021

# CYBERWARFARE

## Week 12 Reading Summary

---

The article *"The Brexit Botnet and User Generated Hyperpartisan News",* is based on a research study done on the usage of botnets, specifically 'Twitter bots' that was used heavily to influence UK's Brexit decisions. The authors explain the steps and ways they took to figure out and separate bots from actual users in the dataset to analyse their proportion. They also outline the problems they encountered recovering and analyzing the deleted tweets and inactive accounts, which is a common behavior of bots after their goals are accomplished. The paper presents a histogram graph indicating the maximum activeness of bots during the voting period as compared to before and after. The report mentions the term 'sock puppet accounts', referring to Twitter accounts. It generally refers to fake accounts created on social media or forums to spread a particular message or agenda with a main goal of influencing public opinion. This is exactly what bots are programmed for. The bots in this particular scenario were subdivided into subnetworks based on their actions or mechanisms – retweeting bot or human generated content, which according to the report, resulted in "different retweet cascades". The authors analyzed the tweets with the following main hashtags "#voteleave, #voteremain, #votein, #voteout, #leaveeu, #bremain, #strongerin, #brexit, and #euref" (page 42). As per their final findings, they concluded that the majority of the tweets generated by botnets inclined towards the leave campaign. Such is the power of botnets to leverage social media and influence people on a large scale. The authors also argued that these bots can be repurposed and modified to fit another campaign in the future.

The research paper *"Common-Knowledge Attacks on Democracy",* discusses the relationship between democracy, autocracy, and cybersecurity practices. It states democracy as an information system and looks at it through an information security point of view. That is to say, democracy as an information system should be defended and a plan or threat model should be implemented for an effective defense. Moreover, the paper classifies two types of knowledge that societies use in their political systems – *common political knowledge*, referring to a common and broader opinion among a group of people with regards to the workings of democracy, and *contested political knowledge*, referring to a disagreement over a particular thing that is debatable in nature. Furthermore, the paper argues that both of them should work in conjunction for the democracy to exist and be stable. However, there exists potential vulnerabilities due to this distinction in knowledge, which other nation states can take advantage of and exploit. They are in particular more vulnerable to information attacks, involving fake news spreading techniques to confuse the public as well as destabilize public confidence. As an instance, Russia was accused of undermining citizens' confidence in the 2016 presidential election. Hence, cybersecurity professionals are encouraged to consider public beliefs as an integral part of defending a system.

***What surprised me?***

I was surprised to know that, according to research, political bots "tweeted at a rate of seven tweets per minute or 929 tweets in 138 min" (Metaxas & Mustafaraj, 2010). I believe this is not a good thing because it would fill the users' feeds with unnecessary and useless tweets every minute. Moreover, the fact that "the more engagement with human agents the botnet generates, the more likely it is to widen cascades beyond the botnet" (page 42) is alarming. This is a growing issue as the bots are becoming increasingly sophisticated and it's going to bring down the value of social media in terms of gaining reliable information.

---

***Questions?***

1. How do Twitter bots differ from the traditional bots used for DDoS attacks? Can Twitter bots be used for DDoS attacks as well?
2. Is freedom of speech and expression in danger with the rise of bots influencing public opinion at a rapid pace?
3. What are some of the threat sources other than nation states that target the democracy of a country with information attacks?

---

***Works Cited***

Bastos, Marco & Mercea, Dan. (2017). The Brexit Botnet and User-Generated Hyperpartisan News. Social Science Computer Review. 37. 089443931773415. 10.1177/0894439317734157.

Farrell, Henry and Bruce Schneier. "Common-Knowledge Attacks on Democracy." (2018).