Expression of interest

Contact details

Country	TURKEY
Name of the organisation	Sabanci University
Name of the contact	Onur Varol
Phone	+90 (537) 701 18 79
Email	onur.varol@sabanciuniv.edu

Specific skills related to the project

Dr. Varol has over 7 years research experience on misbehavior detection and mitigation strategies. He developed a social bot detection system called Botometer. His team ranked top 3 worldwide at the 2015 DARPA Bot Detection Challenge. Efforts on studying social bots yield publications on prestigious venues such as Nature Communications, Communications of the ACM, International Conference of Web and Social Media (ICWSM), and World Wide Web (WWW) conference.

His team at VRL Lab develop projects on detecting accounts manipulating platforms by purchasing fake followers and engagements, utilizing multimodel systems to incorporate image and network information, as well as studying disinformation campaigns of anti-vaccine groups and political manipulation.

For more information you can visit VRL Lab website: http://varollab.com/

Relevant publications

- Varol, O., Ferrara, E., Davis, C., Menczer, F., & Flammini, A. (2017, May). Online human-bot interactions: Detection, estimation, and characterization. In Proceedings of the international AAAI conference on web and social media (Vol. 11, No. 1).
- Varol, O., Ferrara, E., Menczer, F., & Flammini, A. (2017). Early detection of promoted campaigns on social media. *EPJ Data Science*, *6*, 1-19.
- Varol, O., Ferrara, E., Ogan, C. L., Menczer, F., & Flammini, A. (2014, June). Evolution of online user behavior during a social upheaval. In Proceedings of the 2014 ACM conference on Web science (pp. 81-90).
- Varol, O., & Uluturk, I. (2020). Journalists on Twitter: self-branding, audiences, and involvement of bots. Journal of Computational Social Science, 3(1), 83-101.
- Varol, O., & Uluturk, I. (2018). Deception strategies and threats for online discussions. Deception strategies and threats for online discussions by Onur Varol and Ismail Uluturk. First Monday, 23(5-7).

Proposed activities for the project

Proposed activities for the project can lead development of several timely technologies and research outcomes towards understanding foundations to understand motives of people being vulnerable to malicious activities and how to engage with these groups for mitigation. We propose to work on following aims and activities that enable to address these problems.

- Real-time detection of trend topic manipulation
- Develop a multimodal detection system utilizing deep learning technologies to analyze multiple social media platforms
- Conducting online experiments to test effectiveness of mitigation strategies
- Building a taxonomy of misbehaviour strategies and dataset to support research efforts.

Short description of the organisation

Sabanci University (SU) is internationally recognized as one of the most innovative and research-oriented universities in Turkey. According to the results of the World University Rankings 2021 by subject, SU was ranked among top 250 universities in the world and 1st in Turkey both in Computer Science and Social Sciences fields; among top 400 in the world and 2nd in Turkey in Engineering & Technology and among top 800 in the world and 3rd in Turkey in Physical Sciences.

References

Project acronym / starting date	Main objectives	Main activities	Role in the project
SafeNet / 2021 (funded by SU Integration Project)	That project aims to build state-of-the-art methodologies to detect orchestrated activities online and quantify behaviors of human on a controlled social network experiment.	This project has the following objectives: (i) Develop machine learning models to detect malicious user behavior and online conversation by building a robust and generalizable bot and campaign detection system and (ii) experiment on a controlled social network platform to study human behavior under influence of automated agents.	PI
DOISAC / 2016 (funded by Office of Naval Research)	Project name stands for “Detecting Orchestrated Information and Synthetic Account Campaigns”. This project aims at detecting orchestrated information and synthetic activity campaigns on social media using machine learning and computational tools.	In this project, I studied individual and group activities of terrorist recruiters. We build predictive models to identify accounts with malicious intentions and activities.	Researcher
DESPIC / 2012 (founded by DARPA SMISC program.)	Project name stands for “Detecting Early Signature of Persuasion in Information Cascades” and aims to design a system detect persuasion campaigns at their early stage of inception, in the context of online social media.	As part of my PhD, I developed systems that analyses social media data and extracts network, temporal, content, and user-based features to detect online campaigns. I worked on several modules of this framework: (i) a clustering procedure that uses metadata to compute similarity between memes; (ii) a classification system that determines whether a meme is potentially an orchestrated campaign or a genuine, grassroots conversation; (iii) a social bot detection framework called Botometer.	Researcher