AI Based Analysis of the Information Environment for Cybersecurity Applications

Summary

This research develops an AI based digital twin mimicking societal responses to changes in the cybersecurity information environment. The student will enhance their knowledge of information environment analysis and opinion mining and construct a workflow for data gathering from social media and its processing using existing tools for opinion mining. This will result in a database to develop an AI-powered system to measure the influence of an information campaign. The second component is to prototype an AI-powered system to estimate the influence of a planned information campaign, which together would constitute an initial prototype of the proposed digital twin.

Research field:	Information and communication technology
Supervisors:	Dr. Sven Nõmm Dr. Adrian Nicholas Venables
Availability:	This position is available.
Offered by:	School of Information Technologies Department of Software Science
Application deadline:	Applications are accepted between January 01, 2024 00:00 and January 22, 2024 23:59 (Europe/Zurich)

Description

As the Information Environment becomes increasingly interconnected, sentiment analysis and opinion mining of its users have become established disciplines. Widespread social networks have developed into a fertile area for gathering information about reactions to local and global news, advertising campaigns and other marketing events. This has led to both governments and the marketing industry benefitting from research into the understanding, attitudes, and beliefs of a target audience. In these areas, unpredictable changes in the information environment may have a significant effect on how effective an information campaign may be.

Contrary to organised campaigns and other coordinated activities that directly affect the ability to influence an audience, changes in the cybersecurity of a networked infrastructure may have an uncontrolled effect. These may be caused by the actions of a range of different actors, including adversaries, that necessitate counter measures to ensure the continued success of an information campaign. The level of uncertainty in planning an influence campaign requires actions to estimate the potential success of a future information activities. This leads to the major focus and novelty of the proposed doctoral research.

This proposed research targets the development of an AI based digital twin mimicking societal responses to changes in the cybersecurity information environment. Initially, the prospective student will learn and enhance their knowledge of the principles of information environment analysis and opinion mining. This will lead to the construction of a workflow for data gathering from social media and its initial processing using existing tools for opinion mining. This preparation step is expected to result in a sufficiently large database to develop an AI-powered system to measure the influence of the particular information campaign. This is the first novel component of the thesis. The second novel component is to prototype an AI-powered system to estimate the influence of a planned information campaign. Combined together, these components would constitute an initial prototype of the proposed digital twin.

Increasing interest in the use and development of AI-powered tools is leading to transparency in how they function and derive their outputs. This research proposal requires the exploitation of existing tools of explainable AI for the task and their application for each AI-based component. This task leads to a further novel point of the investigation.

Supervisors:

Main Supervisor: Dr. Adrian Venables
Co-Supervisor: Dr. Sven Nõmm

Requirements for the perspective student:

- EU, Australian, Canadian, UK, US or New Zealand citizen.
- Masters degree in computer science or similar area.

- Strong knowledge of mathematics and statistics.
- Strong knowledge of programming: very good experience with Python and packages related to machine learning and deep learning. Experience in using and adapting pretrained models. Preferably supported by public GitHub repositories.
- Knowledge or desire to learn the areas of opinion mining and information environment.
- Perspective candidates asked to develop the proposed idea into an extended research plan of 3-5 pages, single space 12pt and submit it together with the application. The extended plan is expected to demonstrate awareness of the applicant of trends in AI and information environment analysis, planning skills, and the ability to independent thinking.
- Preferable knowledge of the R programming language, scientific publications related to the previous area of research.

Related publications:

Nõmm, Sven; Venables, Adrian (2022). Towards generation of synthetic data sets for hybrid conflict modelling. 15th IFAC Symposium on Analysis, Design and Evaluation of Human Machine Systems, HMS 2022, San José, USA, 12-15 September, 2022. Ed. Zaal, Peter; Schuster, David. Elsevier, 25−30. (IFAC-PapersOnLine; 55-29). DOI: 10.1016/j.ifacol.2022.10.226.

Radsch, Courtney (2022). Artificial Intelligence and Disinformation: State-aligned Information Operations and the distortion of the Public Sphere. Office of the Organization for Security and Co-operation in Europe (OSCE). https://www.osce.org/files/f/documents/e/b/522166.pdf

Price, Kristopher; Nõmm, Sven; Priisalu, Jaan (2019). Analysis of the impact of poisoned data within Twitter classification models. Proceedings of the 5th Interdisciplinary Cyber Research Conference 2019, [ICR] : 29th of June 2019, Tallinn University of Technology. Ed. Osula, Anna-Maria; Maennel, Olaf. Tallinn: Tallinn University of Technology, Department of Software Sciences, 53−57.

Kietzmann, Jan; Paschen, Jeannette; Treen, Emily (2018). Artificial Intelligence in Advertising How Marketers Can Leverage Artificial Intelligence Along the Consumer Journey. Journal of Advertising Research; 263-267. DOI: 10.2501/JAR-2018-035.

To get more information or to apply online, visit https://taltech.glowbase.com/positions/720 or scan the the code on the left with your smartphone.