STAIDCC20: 1st International Workshop on Socio-technical AI Systems for Defence, Cybercrime and Cybersecurity

Stuart E. Middleton
Electronics and Computer Science
University of Southampton
sem03@soton.ac.uk

Anita Lavorgna
Department of Sociology, Social Policy & Criminology
University of Southampton
A.Lavorgna@soton.ac.uk

Ruth McAlister
School of Applied Social and Policy Science
Ulster University
r.mcalister@ulster.ac.uk

ABSTRACT

The purpose of STAIDCC20 workshop is to bring together a mixture of inter-disciplinary researchers and practitioners working in defence, cybercrime and cybersecurity application areas to discuss and explore the challenges and future research directions around socio-technical AI systems. The workshop will showcase where the state of the art is in socio-technical AI, charting a path around issues including transparency, trustworthiness, explaining bias and error, incorporating human judgment and ethical frameworks for deployment of socio-technical AI in the future.

CCS CONCEPTS

•Computing methodologies~Artificial intelligence •Applied computing~Law, social and behavioral sciences~Sociology

KEYWORDS

Artificial Intelligence, Socio-technical, Defence, Cybercrime, Criminology, Cybersecurity

1 Introduction

Law enforcement, cybersecurity and defence applications of AI often involve decision making that can have significant human impact. Such decisions need support from robust tools and intelligence products, where potential for bias, error and missing data is made clear so that decisions made can be both informed and proportionate.

The web is increasingly being used for open source Intelligence (OSINT), with online posts, images and videos being analysed, and data mined, verified and then included as evidence within intelligence products. AI is critical to tackle the extreme volumes of data from the web, allowing filtering, summarizing and modelling for use by human analysts and decision makers. However, AI must be deployed with care and need to be trusted along with the bias/error of results being understood.

Socio-technical AI systems offer the chance for "human in the loop" solutions, overcoming some of the problems associated with black box AI. STAIDCC20 provides a platform for researchers and practitioners to come together, showcasing where the state of the art in socio-technical AI currently is, and identifying as a group the key challenges and future research directions that are most important in the short and medium term for defence, cybercrime and cybersecurity.

WebSci '20 Companion, July 6–10, 2020, Southampton, United Kingdom

ACM ISBN 978-1-4503-7994-6/20/07.
https://doi.org/10.1145/3394332.3402897

2 Workshop Content

STAIDCC20 workshop features a mix of keynotes, presentations of accepted papers and panel led group discussion. We organise two invited keynote talks given by influential researchers from the defence and criminology fields.

Prof Steven Meers: Challenges around Socio-technical AI Systems in Defence: A Practitioners Perspective. This keynote explores the threats and opportunities presented by AI, especially whilst "operationalizing" AI within the Defence enterprise socio-technical perspective. Several practitioner case studies will be covered, with a conclusion reflecting upon the critical role scientists and engineers play in ensuring AI is adopted in a responsible manner that reduces overall harm.

Prof David Wall: AI and Cybercrime: Balancing expectations with delivery! This keynote explores the general issue of using socio-technical AI systems to deal with crime and policing, identifying some of the challenges presented by AI and cybercrime and cybersecurity. It then discusses the wider methodological and socio-political problems of delivering science solutions within a socio-political world, and concludes with a discussion of the practical realities, strengths and weaknesses, of using AI for attribution and investigating cybercrime, and preventing attacks to systems.

Two accepted papers will be presented orally. The first paper, [1] **"Information extraction from the long tail: A socio-technical AI approach for criminology investigations into the online illegal plant trade",** describes an inter-disciplinary socio-technical artificial intelligence (AI) approach to information extraction from the long tail of online forums around internet-facilitated illegal trades of endangered species. It describes a highly iterative methodology, taking entities of interest identified

by a criminologist and using them to direct computer science tools including crawling, searching and information extraction to develop intelligence packages. Two information extraction algorithms are compared, named entity (NE) directed graph visualization and Latent Dirichlet Allocation (LDA) topic modelling, across two case studies involving the online illegal wildlife trade of endangered plants.

The second paper, [2] **"Decoding the Black Box: Interpretable Methods for Post-Incident Counter-terrorism Investigations"**, explores the major challenges of providing explanations of machine learning patterns in human friendly ways to better support decision makers in verifying captured patterns and using them to derive actionable intelligence. A case study is described where a machine learning model predicts possible perpetrators in incidents of terrorism and a variety of interpretability mechanisms are applied to this model to present those patterns in a human understandable manner.

The workshop will host a panel led discussion session, identifying some of the main challenges of socio-technical AI for defence, cybercrime and cybersecurity that exist today, and signposting some positive directions of travel to help inspire future researchers. The workshop panel consists of a mix of practitioners and researchers across the defence, cybercrime and cybersecurity application areas. Representing practitioners, we have **Greg Elliot**, National Cyber Crime Unit (NCCU) National Crime Agency (NCA), **Prof Steven Meers**, Defence Science and Technology Laboratory (DSTL) and **Mark McCluskie**, Nuix, EMEA Head of Investigations. Representing researchers, we have **Prof David Wall**, University of Leeds, Centre for Criminal Justice Studies and **Prof Dame Wendy Hall**, University of Southampton, Electronics and Computer Science.

3 Organisers

The organisers of the workshop have collectively a broad range of expertise in relevant research areas, including artificial intelligence, natural language processing, machine learning, criminology and social science, and expertise in applying them to application areas including defence and cybercrime.

Dr Stuart E. Middleton (workshop chair) is a Lecturer in Computer Science at the University of Southampton. His research focus is on natural language processing and information extraction, often following interdisciplinary approaches utilising socio-technical AI. He is currently the principle investigator of several research grants, including DSTL funded CYShadowWatch (ACC2005442) exploring multi-lingual information extraction from cybercrime forums, and NERC funded GloSAT (NE/S015604/1) examining information extraction from ship logs to support data rescue. He is co-investigator on the FloraGuard project that Anita Lavorgna leads. He was an invited AI expert for the UK Cabinet Office 2019 ministerial AI roundtable on "use of AI in policing" and ATI/DSTL 2019 workshop on "Decision Support for Military Commanders".

Dr Anita Lavorgna is Associate Professor in Criminology at the University of Southampton. She is currently leading the ESRC-funded cross-disciplinary research project FloraGuard on internet-facilitated wildlife trafficking (ES/R003254/1). Anita's research pivots around cybercrimes (especially trafficking activities online), serious and organised crime, and the propagation of misleading and fraudulent health information.

Dr Ruth McAlister is Lecturer in Criminology at Ulster University. Through utilising webscraping, open source intelligence and social network analysis she investigates how digital technology has impacted on criminal activities pertaining to serious and organised crime, exploring how organised networks evolve, diversify and function within cyberspace. Her previous research has examined online recruitment for the purposes of human trafficking, animal rights extremism and child sexual abuse. She is one of the co-investigators on the DSTL funded CYShadowWatch project (ACC2005442).

4 Acknowledgements

This workshop is supported by the Economic and Social Research Council (ES/R003254/1) and UK Defence and Security Accelerator, a part of the Ministry of Defence (ACC2005442). We would like to thank the organizers of the Web Science 2020 conference for agreeing to host our workshop and for their support. All papers submitted to STAIDCC20 received at least three reviews. For this, we would like to thank all reviewers for their time and contributions.

References

[1] Stuart E. Middleton, Anita Lavorgna, Geoff Neumann and David Whitehead. 2020. Information Extraction from the Long Tail: A Socio-Technical AI Approach for Criminology Investigations into the Online Illegal Plant Trade. In Proceedings of ACM Web Science conference (WebSci 2020). ACM, July 6–10, 2020, Southampton, United Kingdom

[2] Ankit Tewari. 2020. Decoding the Black Box: Interpretable Methods for Post-Incident Counter-terrorism Investigations. In Proceedings of ACM Web Science conference (WebSci 2020). ACM, July 6–10, 2020, Southampton, United Kingdom