The Challenges of Socio-Technical AI Systems:
From a Criminological Perspective

Professor David S. Wall, PhD
Cybercrime Group,
Centre for Criminal Justice Studies,
University of Leeds, UK
<d.s.wall@leeds.ac.uk>

ABSTRACT

This short talk will explore the broader issue of using socio-technical artificial intelligence (AI) systems in criminology for responding to cybercrime and cybersecurity issues. It will focus upon the importance of matching the delivery of AI with the scientific (technical) claims for it within a socio-political world. By drawing upon research into cybercrime and cybersecurity (including recent ransomware research), the talk will discuss the realities, the strengths and weaknesses, of using AI with regard to attribution and investigating cybercrime, and also preventing attacks to systems. It will argue that the meanings, logic and understandings of AI systems differ across disciplines which can result in significant differences in expectations. The broad conclusion is that because of this an interdisciplinary approach needs to be taken and that AI it is not a silver bullet. AI systems may be useful, for example, in responding to some cybercrimes, but not others, or effective in addressing aspects of a cybercrime event, such as preventing malware infection; and even then, only with some major caveats. More importantly, is the recognition that AI cannot actually make hard decisions, but it can reasonably inform aspects of the decision-making processes of practitioners, professionals, policy makers and politicians who are mandated to make them. It is not only important to match the delivery of scientific claims with consumer expectations in order to maintain public confidence in the public security sector, but also because an arms races is developing as offenders are also beginning to employ AI in a number of different ways to help them victimise individuals, organisations and nation states[1].

The first part of this talk will draw upon existing examples to explore the general issue of using socio-technical AI systems to deal with crime and policing in a risk society[2][3], before identifying some of the additional challenges presented by AI and cybercrime and cybersecurity[4][5]. The second part will look at the methodological and socio-political problems of delivering science solutions within a socio-political world. The third part will conclude by discussing the practical realities, strengths and weaknesses, of using AI regarding attribution and investigating cybercrime, and preventing attacks to systems.

WebSci'20, July, 2020, Southampton, UK
 978-1-4503-0000-0/18/06...$15.00
https://doi.org/10.1145/xxxxxx

CCS CONCEPTS

Artificial intelligence systems for Cybercrime and Cybersecurity

KEYWORDS

Cybercrimes, Cybersecurity, Ransomware, Data Breaches, Hacking, Policing Cybercrime, Artificial Intelligence

Bio

David S. Wall, PhD is Professor of Criminology in the Centre for Criminal Justice studies, School of Law, University of Leeds, UK where he conducts interdisciplinary research into Cybercrimes and Cybersecurity, Ransomware, Policing Cybercrime, and Organised Cybercrime. He has published a wide range of articles and books on these subjects and has a sustained track record of

interdisciplinary funded research in these areas. He has been a member of various Governmental and UN working groups and he is an Academician of the Academy of Social Sciences (FAcSS) and a Fellow of the Royal Society of Arts (FRSA).

REFERENCES

[1] Wall, D.S. (2018) How Big Data Feeds Big Crime, *Current History: A journal of contemporary world affairs*, January 117(795): 29-34. ISSN 0011-3530 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3359972 http://currenthistory.com/Article.php?ID=1461

[2] Bennett Moses, L. and Chan, J., 2018. 'Algorithmic prediction in policing: assumptions, evaluation, and accountability' *Policing and Society*, 28(7): 806-822.

[3] Edwards, A., 2017. 'Big data, predictive machines and security: The minority report' in M. McGuire and T. Holt (eds), *The Routledge Handbook of Technology*, Crime and Justice. Routledge.

[4] Wall, D.S., 2017. 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing', pp. 1075-1096 in R. Brownsword, E. Scotford and K. Yeung (eds) *The Oxford Handbook of the Law and Regulation of Technology*, Oxford: Oxford University Press.

[5] Porcedda, M.G. and Wall, D.S. (2019) Cascade and Chain Effects in Big Data Cybercrime: Lessons from the TalkTalk hack, *proceedings of WACCO 2019: 1st Workshop on Attackers and Cyber-Crime Operations*, IEEE EuroS&P 2019, Stockholm, Sweden, June 20, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3429958