HUMAN ASPECTS OF AI APPLICATIONS IN CYBERSECURITY AND FORENSICS

Maneka. A. J Wijesekera[1*] & Asanka. P. Sayakkara[2]

[1] Faculty of Graduate Studies, University of Colombo, Sri Lanka

[2] University of Colombo School of Computing, Sri Lanka

*Corresponding author: maneka.wijesekera@gmail.com

Abstract

Law enforcement agencies are starting to rely on artificial intelligence (AI) to detect cyber threats, investigate digital crimes and analyse forensic evidence. Most research on these tools looks at how well they perform technically, or at adoption in other sectors and in Western policing. We know little about how Sri Lankan law enforcement professionals perceive, trust and use AI in cybersecurity and digital forensics work, or how local organisational and governance conditions affect that use. This study addresses that gap with investigators, cybersecurity analysts, intelligence personnel and digital forensics specialists in Sri Lanka. By "AI tools" we mean AI-enabled systems used in investigations, such as automated threat detection, anomaly analysis and forensic triage tools, and we also record how much each participant actually uses them.We combine four frameworks in one conceptual model. The Technology Acceptance Model contributes perceived usefulness and ease of use. Trust in Automation Theory contributes reliability, transparency and calibrated trust. Socio-Technical Systems Theory covers organisational structure, workflow and accountability, and Responsible AI principles cover ethical concern and governance. The model shows how these constructs relate and which will be tested statistically and which explored through interviews.The design is explanatory sequential mixed methods. In the first phase, a survey of about 200 officers, recruited by purposive sampling stratified by role, tests relationships between the constructs and actual AI use. In the second phase, semi-structured interviews with selected survey respondents help explain the results: how trust forms in practice, how officers handle accountability when AI informs a decision, and what they do when an AI explanation is inadequate. The study aims to describe the human and organisational factors linked to well-calibrated reliance on AI in Sri Lankan law enforcement and to inform training and governance. Findings will be reported without assuming in advance which barriers matter most.

Keywords: Artificial Intelligence, Digital Forensics, Trust, Human-Centered AI, Law Enforcement