Implementing Cyber Threat Intelligence in Dark Web Cybercrime Prediction

Xue Ling Teh

RMPP_PCOM7E June 2023 - Research Methods and Professional Practice

Current Landscape

- Forensics and criminology research contribution
- Cybercriminal profiling
  - Individual/group motives
- Reinforce cybersecurity organization reputation
- Security welfare of netizens

Research Question

How has the implementation of cybersecurity techniques – particularly CTI – contributed towards cybercrime prediction in the dark web and what are potential gaps in mitigating future cybercrime?

Aims and Objectives

01

Evaluate existing literature

Literature that closely explores CTI implementation and/or dark web cybercrime prediction

02

Determine strengths, limitations and gaps

Current research's strengths, limitations and gaps

03

Identify CTI integration challenges

Potential challenges in integrating CTI into dark web cybercrime predictive modelling

01

Literature Design

Key literature, research design and strategy

Key Literature

(Schäfer et al., 2019)

CTI

Cyber Threat Intelligence sources, framework (e.g. BlackWidow)

(Horan & Saiedian, 2021; Basheer & Alkhatib, 2021)

Dark web

Hidden, unindexed, anonymous, limited traceability

STRIDE

Threat model

Cybercrime prediction

Predicting cybercrime trend

Methodology

02

Security Compliance

Ethics, compliance and risk management

Ethical Considerations

03

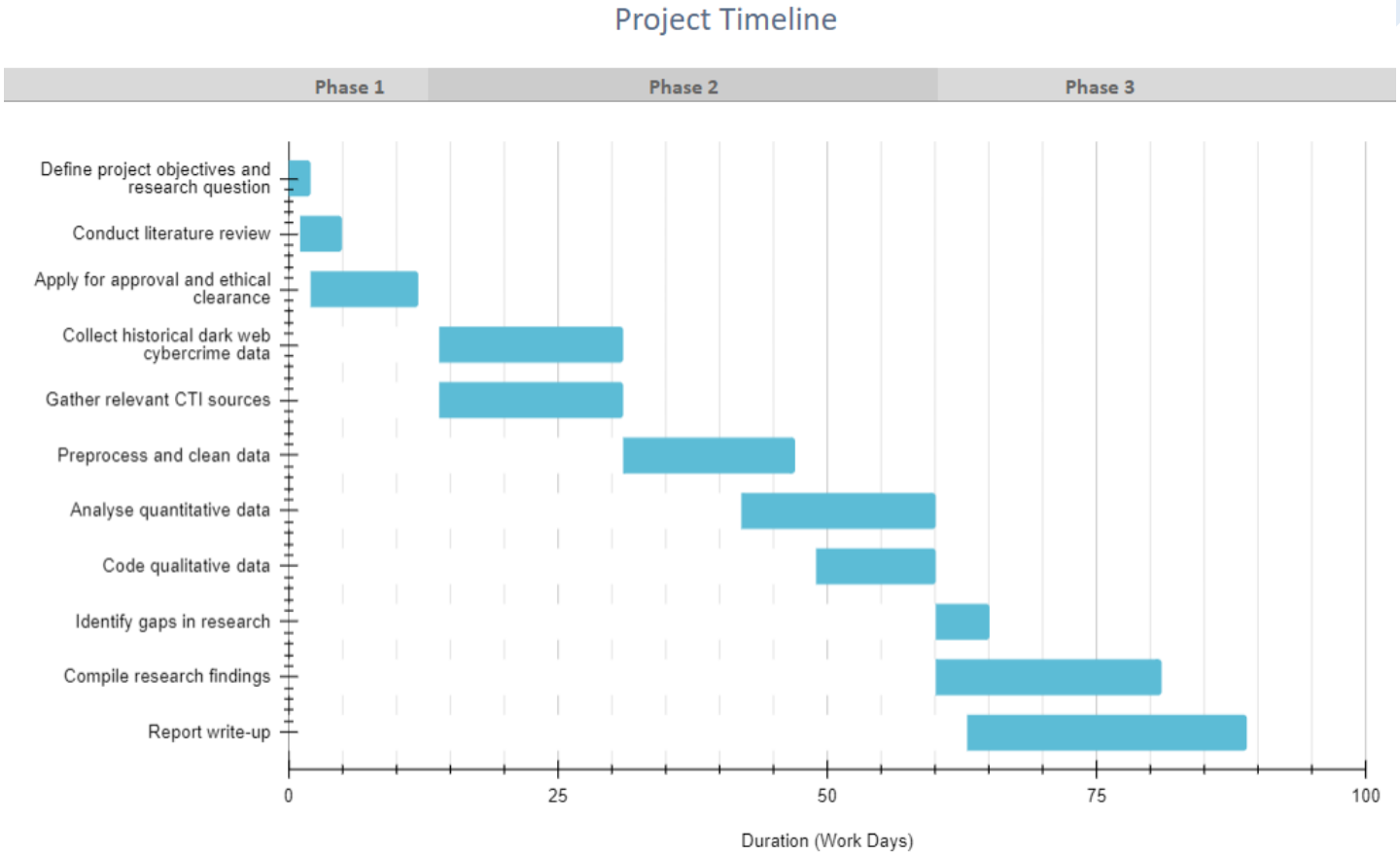
Deliverables

Proposed artefacts and timeline

Applicable Artefacts

Artefact		Description
	**Coded qualitative analysis data**	Theme, keyword analysis from unstructured open-ended data (Adu, 2019)
	**CTI Knowledge Graph**	Mapping relationships between actors, topics (Schäfer et al., 2019)

Proposed Timeline



References (1)

- Adu, P. (2019) *A step-by-step guide to qualitative data coding*. Routledge.
- Basheer, R. & Alkhatib, B. (2021) Threats from the dark: A review over Dark Web Investigation Research for Cyber Threat Intelligence, Journal of Computer Networks and Communications. *Journal of Computer Networks and Communications* 2021: 1-21. DOI: https://doi.org/10.1155/2021/1302999
- Bezerra, J., César, C., de Souza, N., & Hirata, C. (2020) Extending STPA with STRIDE to identify cybersecurity loss scenarios. *Journal of Information Security and Applications*, 55: 1-13.

References (2)

- Dawson, C. (2015) *Projects in Computing and Information Systems: A Student's Guide*. Harlow: Pearson.
- Horan, C. & Saiedian, H. (2021) Cyber crime investigation: Landscape, challenges, and future research directions. *Journal of Cybersecurity and Privacy* 1(4): 580-596. DOI: https://doi.org/10.3390/jcp1040029
- Information Commissioner's Office (ICO) (N.D.) Guide to the General Data Protection Regulation (GDPR).
- Open Web Application Security Project (OWASP). (2021) OWASP Top Ten. Available from: https://owasp.org/www-project-top-ten/ [Accessed 10 August 2023].

References (3)

- Schäfer, M., Fuchs, M., Strohmeier, M., Engel, M., Liechti, M. & Lenders, V. (2019) May. BlackWidow: Monitoring the dark web for cyber security information. *2019 11th International Conference on Cyber Conflict (CyCon).* 28-31 May. IEEE. 1-21.

- Tate, J.A. & Happ, M.B. (2018) *Qualitative Secondary Analysis: A case exemplar*, *Journal of pediatric health care : official publication of National Association of Pediatric Nurse Associates & Practitioners*. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5911239/ [Accessed 18 August 2023].