Literature Review: Implementing Cyber Threat Intelligence in Dark Web Cybercrime Prediction

Xue Ling Teh

Student ID: 12690175

Research Methods and Professional Practice: Unit 7

Contents

Introduction

The dark web has become a thriving hub for cybercriminal activities, posing significant challenges to cybersecurity professionals, researchers, and law enforcement agencies particularly specialising in forensics and criminology. In response to this escalating threat landscape, implementing Cyber Threat Intelligence (CTI) has emerged as a promising cybersecurity strategy for enhancing dark web cybercrime prediction. This critical analysis literature review aims to evaluate the existing body of literature that explores the implementation of CTI in dark web cybercrime prediction. By examining the strengths, limitations, and gaps in the current research, this review seeks to shed light on the effectiveness and potential challenges of integrating CTI into predictive models for combatting cybercrime in the dark web.

A combination of secondary quantitative and qualitative analysis (Tate & Happ, 2018) are utilised in the evaluation of the relevant literature case studies. Learning to recognise the characteristics of cybercrime by devising methods to mitigate the negative effects of cybercrime helps prevent future victims and protect current end users, hence strengthening the reputation of cybersecurity organisations.

Cybercrime in the Dark Web

Cyber terrorism poses a significant international threat due to its potential to cause widespread harm quickly globally, especially via an elusive environment such as the dark web. The hidden part of the Internet, unindexed by search engines and accessible via custom URL is the deep web. Within the deep web is the dark web, where cybercrimes

are prevalent due to the nature of anonymity and limited traceability. (Horan & Saiedian, 2021; Basheer & Alkhatib, 2021)

Table 1 shows an overview of the international jurisdictions, including international, regional, and local organisations that are involved in establishing cyber regulations and resolving global threats, such as cyber terrorism.

Table 1: Organisations Regulating Multi-Jurisdiction on Global Crimes

Scope	*Organisation*
International	United Nations
	Interpol
	Council of Europe Convention on Cyber Crime
Regional	Council of Europe
	International Multilateral Partnership against Cyber Terrorism (IMPACT)
	Association of Southeast Asian Nations (ASEAN)
	Asia-Pacific Economic Cooperation (APEC)

Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence (CTI) can be classified into three levels: strategic, operational, and tactical (Basheer & Alkhatib, 2021):

1. Strategic intelligence identifies threat sources and their purpose and is often associated with Advanced Persistent Threats (APT).

2. Operational intelligence gathers information on the Tactics, Techniques, and Procedures (TTP) of threat actors, through threat hunting.
3. Tactical, also known as technical intelligence, focuses on threat actors' real-time approaches and guidance on defensive countermeasures for Indicators of Attack (IOA) and Indicators of Compromise (IoC).

The threat intelligence lifecycle is guided by phases (Cascavilla et al., 2021). CTI begins with collecting data from a wide range of sources, including open-source intelligence (OSINT), closed-source intelligence such as proprietary threat feeds from cybersecurity vendors, and intelligence sharing platforms and forums. Arnold et al. (2019) describes a great overview of a Dark-Net CTI tool. The collected data is then analyzed to identify patterns, trends, and potential indicators of upcoming cybercriminal activities. This involves using various data analysis techniques, such as data mining, machine learning, and natural language processing, to uncover hidden insights. Cyber threat intelligence analysts may proactively search for potential threats and adversaries on the dark web. They search for discussions related to specific keywords, malware types, or targeted industries to identify potential cybercrime campaigns in their early stages. Understanding vulnerabilities in software and systems is crucial for predicting potential cybercrime. Cyber threat intelligence can provide insights into the exploitation of new or zero-day vulnerabilities that may surface on the dark web. Implementing early warning systems that alert organizations to potential cyber threats can help them take proactive measures to defend against upcoming attacks. Cyber threat intelligence is an ongoing process. Continuously monitoring the dark web and updating threat intelligence allows for real-time response to emerging threats. The majority of CTI originate from unstructured data such

as incident reports. Based on the identified cyber threats, organizations can develop and refine their incident response plans to ensure they are prepared to handle potential security incidents.

CTI in Enhancing Dark Web Cybercrime Prediction

This section examines the empirical evidence from existing case studies on the effectiveness of CTI in improving dark web cybercrime detection and unstructured crime prediction (Rawat et al., 2021) . Real-world applications of CTI, evaluating their impact on threat detection, response times, and incident prevention through actionable intelligence. An instance where CTI implementation has led to successful mitigation of cyber threats on the dark web was using the BlackWidow analysis tool (Schäfer et al., 2019).

There are a variety of methodologies applicable in predictive modelling in criminology, including the use of data mining, machine learning, and criminal profiling. The initial step of criminal profiling is determining whether they are insider or external threat actors, which can be deduced via their characteristics and behaviour patterns, in which the threat actor profile can be matched to threat actor groups and the cybercrimes the group are well-known for. Implementing CTI enables the enrichment of data, including deviation detection such as outlier analysis. Monitoring dark web forums, marketplaces, and chat rooms provides insights into potential cybercriminal activities, including the buying and selling of stolen data, exploit kits, and malicious software (Schäfer et al., 2019).

Future of Cybercrime Prediction

CTI has witnessed groundbreaking development which evolved over the years and enhanced the existing cybercrime detection and prediction capabilities. The key gaps lie in the complexities of analysing unstructured data, the potential for false positives and negatives, and the difficulty of validating dark web-sourced information. Therefore, proposed avenues for future research include improving data collection and synthesis methodologies while addressing legal and ethical concerns in relation to data privacy, developing hybrid CTI models, and devising a reliable standard of validating a system's security posture.

References

Arnold, N., Ebrahimi, M., Zhang, N., Lazarine, B., Patton, M., Chen, H. & Samtani, S. (2019) 'Dark-Net Ecosystem Cyber-Threat Intelligence (CTI) Tool', *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Shenzhen, China, 01-03 July. IEEE. 92-97.

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

Cascavilla, G., Tamburri, D.A. & Van Den Heuvel, W.J. (2021) Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security* 105(102258): 1-29. DOI: https://doi.org/10.1016/j.cose.2021.102258

Dawson, M. (2015) *New threats and countermeasures in digital crime and cyber terrorism*. IGI Global.

Healey, M., Matthews, K., & Cook-Sather, A. (2020) *Writing about learning and teaching in higher education: Creating and contributing to scholarly conversations across a range of genres*. Center for Engaged Learning Open-Access Books, Elon University. 142-152.

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

Kure, H. & Islam, S. (2019) Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. *Journal of Universal Computer Science 25*(11): 1478-1502.

Rawat, R., Rajawat, A.S., Mahor, V., Shaw, R.N. & Ghosh, A. (2021) Dark web—onion hidden service discovery and crawling for profiling morphing, unstructured crime and vulnerabilities prediction. *Innovations in Electrical and Electronic Engineering: Proceedings of ICEEE 2021*: 717-734. Springer Singapore.

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 27 July 2023].

Taylor, R.W., Fritsch, E.J., Liederbach, J., Saylor, M.R. & Tafoya, W.L. (2019) *Cyber crime and cyber terrorism*. New York, NY: Pearson.