Actionable Open-source Intelligence Architecture for Cold Case Investigations

Swikar Bhandari

University of Twente, Drienerlolaan 5, 7522 NB Enschede, Netherlands

Abstract

The number of unsolved homicides in the Netherlands has gradually stacked up over the past few decades resulting in more than 1700 "cold cases" as of 2024. To tackle this problem, this paper presents a socio-technical system that facilitates the semi-automated collection and derivation of actionable intelligence from publicly available information for cold case investigations. The proposed system is designed using a multi-disciplinary approach by integrating solutions from the domains of homicide, ethics and philosophy, intelligence studies and computer science. Additionally, existing requirement engineering literature was used to identify the necessary requirements needed to design the proposed system. Thereby ensuring the safety, security and responsible use of OSINT for cold case investigations. We hope that the proposed socio-technical system can help mitigate cold cases and thus contribute towards the social good.

Keywords

OSINT, cold case, actionable intelligence, socio-technical system, requirements engineering

1. Introduction

Homicide can fundamentally be understood as the act of killing a human being either intentionally (murder) or non-intentionally (manslaughter). In context to the Netherlands, around 160 homicides occur every year on average [1]. Despite police investigation, not all homicides are solved mainly due to lack of intelligence, evidence or tunnel vision [2]. The unsolved homicides that are no longer under active police investigation are commonly referred to as "cold cases" [3]. As a result, the number of unsolved homicides in the Netherlands has gradually stacked up over the past few decades resulting in more than 1700 unsolved "cold cases" as of 2024.

Fortunately, there are different non-law enforcement stakeholders that aid law enforcement by participating in cold case investigations through activities such as citizen science or crowdsourcing. Both the police and non-law enforcement stakeholders conduct cold case investigations by relying on the information that is openly available to the public that is referred to as publicly available information (PAI) or open-source information (OSINF). The intelligence derived from PAI or OSINF is known as open-source intelligence (OSINT). Over the years, OSINT has shown its potential in the domain of policing and law enforcement, from identifying criminal behaviour to providing supporting evidence in court [4]. However, the existing literature lacks adequate research on potential of OSINT for homicide investigations.

In context to OSINT, there are several issues that must be addressed to ensure its suitability for cold case investigations. First, OSINF about homicides is not primarily disseminated for investigation purposes. Therefore, relevant information must be identified and extracted from the big heap of available OSINF about homicides that can be considered suitable for conducting investigations. Second, relying on OSINT also raises a number of epistemic issues such as unreliability, inconsistency and fuzziness [5]. Third, there are various legal and ethical issues associated with OSINT. For example, automated data collection at a large scale may even slow down and crash the website due to huge amount of web traffic.

In: M. Abbas, F. B. Aydemir, M. Daneva, R. Guizzardi, J. Gulden, A. Herrmann, J. Horkoff, M. Oriol Hilari, S. Kopczyńska, P. Mennig, E. Paja, A. Perini, A. Rachmann, K. Schneider, L. Semini, P. Spoletini, A. Vogelsang. Joint Proceedings of REFSQ-2025 Workshops, Doctoral Symposium, Posters & Tools Track, and Education and Training Track. Co-located with REFSQ 2025. Barcelona, Spain, April 17, 2025.

s.b.bhandari@utwente.nl (S. Bhandari)

0009-0007-0824-5255 (S. Bhandari)

Extracting information without the permission of the source may lead to legal consequences such as breach of contract and copyright infringement.

Similarly, facilitating a collaboration between the police and non-law enforcement stakeholders for criminal investigations have demonstrated to have significant risks [6]. For example, citizens who lack necessary training and expertise have shown to cross the boundary between boundary between police and citizen territory by performing tasks such as arresting or interrogating people based on their own suspicions, breaking chain of custody [7].

The goal of investigation is to derive actionable intelligence that serve as evidence to reopen existing cold cases. Thus, it is important to understand that while evidence can always provide some degree of intelligence the reverse is not the case [4]. If proper standards or guidelines are neglected then despite having actionable intelligence, the decision maker cannot use the intelligence as evidence, thereby compromising the investigation [8].Therefore, it is necessary to address these challenges before introducing a socio-technical solution, especially for a high-risk domain such as cold case investigations.

Past experiences have already demonstrated the consequences of introducing socio-technical solutions in the domain of policing and law enforcement without critically reflecting their impact towards society. For example, the fraud tackling tool called SyRI that was used by the Dutch government, violated many ethical guidelines including the right to privacy according to article 8 of the European Convention on Human Rights [9, 10]. Existing requirements engineering (RE) approaches have helped stakeholders to effectively to develop solutions in domain of policing and law enforcement. However, the current RE literature lacks adequate research on addressing AI-driven and ethical requirements [11].

In light of the above research gaps and challenges, this PhD project aims to design a socio-technical system that facilitates a collaboration between various non-law enforcement stakeholders and the police to semi-automatically collect PAI and derive actionable intelligence to aid in the forensic investigation of cold cases. Similarly, the proposed system will be designed to ensure the safety, security and responsible use of OSINT for cold case investigations.

2. Related Work

There are several studies that have demonstrated the implementation of requirement engineering (RE) to develop solutions in the domain of policing and law enforcement. The existing RE literature depicts a heavy emphasis on crimes associated with the cyber security domain including fraud, identity theft, spam [12, 13, 14, 15, 16, 17, 18]. Most studies have also focused on identifying requirements associated with digital investigations [19, 20, 21, 22, 23, 24]. Similarly, few studies have explored the challenges associated with crowdsourcing [24, 18]. However, to the best of author's knowledge, there have been no RE studies focused on homicide investigations.

In context to RE methods or approaches, goal-oriented requirements engineering (GORE) method has been used in two studies associated with digital investigations [19, 20]. Similarly, agile method was implemented by [16] and [25] to combat crimes associated with cyber-attacks and illegal timber trades respectively. [26] combined the principles of RE and criminology to develop profile of attackers for software-intensive systems. [27] used a design science approach to develop an ethics and privacy-based system dedicated for maritime surveillance. Scenario-based approach was used by to conduct requirement elicitation for tackling fraud. However, several studies have implemented unique approaches to identify requirements without solely relying on a single RE method [21, 28, 29, 26, 23, 13, 30]. For instance, a multi-faced approach was implemented to develop crime records management system for the Uganda police force [30].

Most of the requirements addressed in the current literature in the domain of policing and law enforcement consists of crime, security requirements. However, the rise of artificial intelligence (AI) has brought forth novel hurdles including ethical challenges that must be addressed to when developing AI-driven solutions [11]. Although there are few studies that have already attempted to address the AI-driven and ethical requirements [27, 11], there is still a lack of sufficient research in this topic.

3. Methodology

This PhD project tackles the underlying problem of cold cases through a multi-disciplinary approach by integrating solutions from the domains of homicide, ethics and philosophy, intelligence studies as well as computer science. Similarly, this project relies on the existing RE literature to identify various requirements required to design the proposed system. This PhD project therefore focuses on finding answers to the following research questions:

RQ1. How can relevant information required for cold case investigations be extracted from OSINF?
The first step involved understanding the domain of homicide investigations and OSINT. The project partners involved in this PhD such as the Technology for Criminal Investigations (TCI) research group at the Saxion University of Applied Science (UAS) and the Police Academy of the Netherlands enabled the opportunity to collaborate with experts in the domains of homicide and cold case investigations. Additionally, this collaboration also provided the opportunity to undertake OSINT training at the International Anti Crime Academy (IACA).

To enable investigators, tackle the problem of tunnel vision caused due to the lack of intelligence during criminal investigations, a new method known as scenario-based methods has been developed over the past decades [2]. A scenario is a story that describes foreseeable interactions between characters and the system. This approach involves analysing a criminal incident by finding the answer to the question of "what happened during the incident?" by using various scenario components. One of the well-known scenario-based approach is known as the narrative approach developed by Prof. Peter de Kock. It involves developing a scenario using twelve dynamically connected building called the Elementary Scenario Components (ESCs) [5]. This approach was used to develop a system called Pandora to conduct terrorist investigations and has already shown promising results.

In 2020, the "Cold Case: Solved Unsolved" project adapted de Kock's model with some modifications to make it suitable for homicide investigations [31]. However, the empirical validity of the narrative approach for cold case investigations has not been established yet.

In this project, the adaptation of narrative approach developed during the cold and unsolved project was evaluated to determine its empirical validity based on the existing literature on homicide studies. The findings of the evaluation are used to improve the current model through the addition of essential components and removal of unsuitable or problematic components for homicide investigations, respectively.

After this step, the adjusted version of the narrative approach was used to semi-automatically collect, analyse and derive OSINT about cold cases through a human-machine collaboration. First, an academic law enforcement collaboration was facilitated to conduct OSINT driven-cold case investigations through the students enrolled at the "Cold Case Minor" course. This course is delivered by the TCI research group which is a collaboration between Saxion UAS and Police Academy of the Netherlands.

Similarly, the potential of the latest technological advancements in automated (AI-based) information extraction was evaluated through unstructured text using Large Language Models (LLMs). The information collected in this step was further used to develop and evaluate scenarios.

RQ2. What are the normative requirements that justifies OSINT as actionable or non-actionable for cold case investigations?
To become familiar with the domain of ethics and philosophy, the course "Machines, minds, and society: the ethics and epistemology of AI" was undertaken at the University of Twente. After that, the evaluation of OSINT was conducted to determine the normative criteria for actionability using the "ethics through epistemology" approach. This process was helped understand the epistemic, ethical and legal challenges associated with OSINT in context to cold case investigations [32].

RQ3. How can we address the epistemic challenges associated with OSINT for cold case investigations?
To address the epistemic challenges associated with OSINT, the academic law enforcement collaboration was further implemented by operating student analysts to conduct the reliability assessment of OSINT

for cold case investigations. The assessments were conducted using information quality metrics such as source credibility and information reliability based on the NATO STANAG 2511 scales [33].

The next step involves the representation and analysis of scenarios using 2 approaches. The first approach involves representing the complex scenarios using knowledge graphs (KG). A KG is a visual representation of knowledge in a graph-based structure through entities and relationships. KGs enable investigators to visually analyse the uncertainty associated with scenarios developed from OSINT. Similarly, the second approach involves using a probabilistic database system called Dubio that enables the storage, querying and manipulation of uncertain information [34].

RQ4. How can the challenges associated with the involvement of non-law enforcement stakeholders in cold case investigations be addressed?
In context to cold case investigation, unidentified perpetrators may voluntarily participate in these initiatives to gather the information that police possess and finds ways to mislead or disrupt the investigation. Thus, several strategies were implemented to prevent this while facilitating an academic law enforcement collaboration. First, the background information of all participants was evaluated alongside any conflict of interest regarding any case they investigated. Similarly, the participants were provided with necessary theoretical knowledge and practical skills from experts. For example, IACA provided OSINT training to participants through with they learned how to use state of art tools to conduct OSINT investigation and document their findings. Lastly, information collected by participants were validated to ensure data integrity.

The theoretical and practical findings generated from the research questions will be further evaluated to find the answer to the broader research question: **To what extent can the proposed socio-technical system harness the power of OSINT to aid in the forensic investigation of cold cases?**

4. Proposed solution

Using a multi-disciplinary approach described in the previous section, the proposed actionable OSINT architecture for cold case investigations was developed. Figure 1 shows a system context diagram of the proposed architecture to demonstrate the interaction of stakeholders with the different components of OSINT system to derive actionable intelligence. The system begins with the extraction of OSINF using the narrative approach through both human and machine-based approaches. The next step consists of evaluating the reliability of OSINF collected in the previous step using information analysts.

In the third step, the system will derive and represent plausible scenarios using the information collected and evaluated in the previous steps. The selected scenarios will be then analysed by both non-law enforcement and law enforcement decision makers. If the intelligence seems promising, it will further be verified and validated using closed source intelligence to determine whether the derived OSINT can be considered actionable or non-actionable. The cold case will only be recommended to be re-opened if the derived intelligence proves to be actionable.

5. Research Progress and Future Work

The first year of the PhD focused on understanding the multi-disciplinary domains. In the second year, the empirical evaluation and improvement of the narrative approach for homicide investigations was conducted. The initial findings of this study were presented on the Homicide Research Working Group 2023 annual conference. Similarly, the normative evaluation of OSINT was conducted to using the "ethics through epistemology" approach to determine the actionability of OSINT for cold case investigations [32]. These steps served as the foundation that helped identify the different requirements necessary to develop the proposed system. The findings of the first step were further used to develop the data collection plan to facilitate a human-machine collaboration. Lastly, the reliability assessment of OSINT for cold case investigations has been completed.

Currently, the research is focused on exploring different approaches to represent the collected information using knowledge graph and probabilistic data integration approaches. This will help find

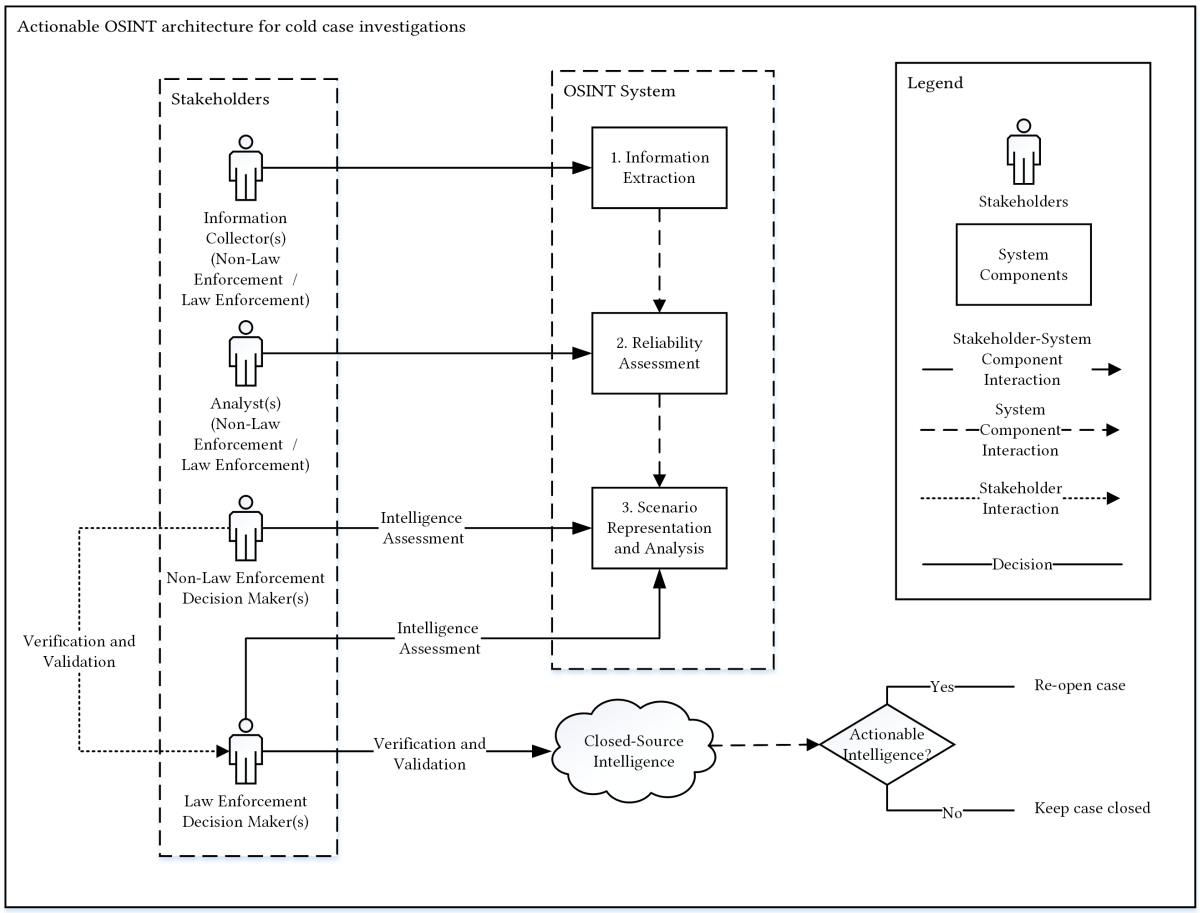

Figure 1: System context diagram of actionable OSINT architecture for cold case investigations

an answer to RQ3. After the completion of this step, both the theoretical and findings will be evaluated to answer the main research question: "To what extent can the proposed socio-technical system aid in the forensic investigation of cold cases?"

6. Conclusion

In this paper, we propose a socio-technical solution to conduct OSINT-driven cold case investigations. The proposed system facilitates a collaboration between various non-law enforcement stakeholders and the police to semi-automatically collect PAI and derive actionable intelligence to aid in the forensic investigation of cold cases. The proposed solution is designed using a novel multi-disciplinary approach by integrating solutions from the domains of homicide, ethics and philosophy, intelligence studies and computer science. Similarly, this project draws upon the existing RE literature to identify various requirements needed to design the proposed system. Additionally, this project contributes to the existing RE literature by addressing the research gap concerning AI-driven and ethical requirements. We hope that this project can contribute towards the reduction of cold cases and help deliver justice to the victims alongside their close ones. Thereby, contributing towards the social good and paving a path towards the development of a safe society.

Acknowledgments

This research project is supported by the research grant from the Dutch Centrum voor Veiligheid en Digitalisering. The author is thankful for all the support provided by the supervisors involved in this

project from the University of Twente, Saxion University of Applied Sciences and the Police Academy of the Netherlands.

References

[1] CBS, Male homicide rate up in 2021, 2022. URL: https://www.cbs.nl/en-gb/news/2022/39/male-homicide-rate-up-in-2021.

[2] C. Epskamp-Dudink, J. Winter, Benefits of scenario reconstruction in cold case investigations, Journal of Criminal Psychology 10 (2020) 65–78. doi:10.1108/JCP-09-2019-0035.

[3] J. M. Adcock, S. L. Stein, Cold Cases: Evaluation Models with Follow-up Strategies for Investigators, Second Edition, 2 ed., Routledge, New York, 2014. doi:10.1201/b17698.

[4] F. Sampson, Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings, The Police Journal 90 (2017) 55–69. doi:10.1177/0032258X16671031.

[5] P. de Kock, Anticipating criminal behaviour: Using the narrative in crime-related data, Doctoral Thesis, Tilburg center for Cognition and Communication (TiCC), Tilburg, 2014.

[6] R. Granja, Citizen science at the roots and as the future of forensic genetic genealogy, International Journal of Police Science & Management (2023). doi:10.1177/14613557231164901.

[7] A. Mols, J. Pridmore, When Citizens Are "Actually Doing Police Work": The Blurring of Boundaries in WhatsApp Neighbourhood Crime Prevention Groups in The Netherlands, Surveillance & Society 17 (2019) 272–287. doi:10.24908/ss.v17i3/4.8664.

[8] S. Ramwell, T. Day, H. Gibson, Use Cases and Best Practices for LEAs, in: B. Akhgar, P. S. Bayerl, F. Sampson (Eds.), Open Source Intelligence Investigation, Springer International Publishing, Cham, 2016, pp. 197–211. doi:10.1007/978-3-319-47671-1_13.

[9] L. Strikwerda, Predictive policing: The risks associated with risk assessment, The Police Journal 94 (2021) 422–436. doi:10.1177/0032258X20947749.

[10] X. van Bruxvoort, M. van Keulen, Framework for Assessing Ethical Aspects of Algorithms and Their Encompassing Socio-Technical System, Applied Sciences 11 (2021) 11187. doi:10.3390/app112311187.

[11] K. Ahmad, M. Bano, M. Abdelrazek, C. Arora, J. Grundy, What's up with Requirements Engineering for Artificial Intelligence Systems?, in: 2021 IEEE 29th International Requirements Engineering Conference (RE), 2021, pp. 1–12. doi:10.1109/RE51729.2021.00008.

[12] B. Whitworth, E. Whitworth, Spam and the social-technical gap, Computer 37 (2004) 38–45. doi:10.1109/MC.2004.177.

[13] H. Dehghanniri, E. Letier, H. Borrion, Improving security decision under uncertainty: A multi-disciplinary approach, in: 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015, pp. 1–7. doi:10.1109/CyberSA.2015.7166134.

[14] T. Grant, Specifying functional requirements for simulating professional offensive cyber operations, 2015.

[15] A. S. Yesuf, L. Wolos, K. Rannenberg, Fraud Risk Modelling: Requirements Elicitation in the Case of Telecom Services, in: S. Za, M. Drăgoicea, M. Cavallari (Eds.), Exploring Services Science, volume 279, Springer International Publishing, Cham, 2017, pp. 323–336. doi:10.1007/978-3-319-56925-3_26.

[16] E. Hadar, A. Hassanzadeh, Big Data Analytics on Cyber Attack Graphs for Prioritizing Agile Security Requirements, in: 2019 IEEE 27th International Requirements Engineering Conference (RE), 2019, pp. 330–339. doi:10.1109/RE.2019.00042.

[17] D. Cirqueira, D. Nedbal, M. Helfert, M. Bezbradica, Scenario-Based Requirements Elicitation for User-Centric Explainable AI: A Case in Fraud Detection, in: A. Holzinger, P. Kieseberg, A. M. Tjoa, E. Weippl (Eds.), Machine Learning and Knowledge Extraction, volume 12279, Springer International Publishing, Cham, 2020, pp. 321–341. doi:10.1007/978-3-030-57321-8_18.

[18] H. Rosser, M. Mayor, A. Stemmler, V. Ahuja, A. Grover, M. Hale, Phish Finders: Crowd-powered

RE for anti-phishing training tools, in: 2022 IEEE 30th International Requirements Engineering Conference Workshops (REW), 2022, pp. 130–135. doi:10.1109/REW56159.2022.00031.

[19] B. Aziz, C. Blackwell, S. Islam, A Framework for Digital Forensics and Investigations: The Goal-Driven Approach, International Journal of Digital Crime and Forensics (IJDCF) 5 (2013) 1–22. doi:10.4018/jdcf.2013040101.

[20] J. C. Deprez, C. Ponsard, N. Matskanis, A Goal-Oriented Requirements Analysis for the Collection, Use and Exchange of Electronic Evidence across EU Countries, in: 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW), 2016, pp. 106–113. doi:10.1109/REW.2016.033.

[21] J. Gray, V. N. L. Franqueira, Y. Yu, Forensically-Sound Analysis of Security Risks of Using Local Password Managers, in: 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW), 2016, pp. 114–121. doi:10.1109/REW.2016.034.

[22] C. Rudolph, Exploring the Space of Digital Evidence – Position Paper, in: J. K. Liu, R. Steinfeld (Eds.), Information Security and Privacy, volume 9722, Springer International Publishing, Cham, 2016, pp. 249–262. doi:10.1007/978-3-319-40253-6_15.

[23] F. Rivera-Ortiz, L. Pasquale, Towards Automated Logging for Forensic-Ready Software Systems, in: 2019 IEEE 27th International Requirements Engineering Conference Workshops (REW), IEEE, Jeju Island, Korea (South), 2019, pp. 157–163. doi:10.1109/REW.2019.00033.

[24] M. Bano, D. Zowghi, Crowd Vigilante, in: M. Kamalrudin, S. Ahmad, N. Ikram (Eds.), Requirements Engineering for Internet of Things, volume 809, Springer Singapore, Singapore, 2018, pp. 114–120. doi:10.1007/978-981-10-7796-8_9.

[25] I. N. Athanasiadis, D. Anastasiadou, K. Koulinas, F. Kiourtsis, Identifying Smart Solutions for Fighting Illegal Logging and Timber Trade, in: J. Hřebíček, G. Schimak, M. Kubásek, A. E. Rizzoli (Eds.), Environmental Software Systems. Fostering Information Sharing, volume 413, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 143–153. doi:10.1007/978-3-642-41151-9_14.

[26] N. Hussein, W. Wang, J. L. Nedelec, X. Wei, N. Niu, Unified Profiling of Attackers via Domain Modeling, in: 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW), 2016, pp. 98–101. doi:10.1109/REW.2016.031.

[27] J. Rajamäki, Design Science Research Towards Ethical and Privacy-Friendly Maritime Surveillance ICT Systems, in: T. Tagarev, K. T. Atanassov, V. Kharchenko, J. Kacprzyk (Eds.), Digital Transformation, Cyber Security and Resilience of Modern Societies, volume 84, Springer International Publishing, Cham, 2021, pp. 95–115. doi:10.1007/978-3-030-65722-2_7.

[28] T. Tun, B. Price, A. Bandara, Y. Yu, B. Nuseibeh, Verifiable Limited Disclosure: Reporting and Handling Digital Evidence in Police Investigations, in: 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW), 2016, pp. 102–105. doi:10.1109/REW.2016.032.

[29] H. Dehghanniri, H. Borrion, Toward a More Structured Crime Scripting Method, in: 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW), 2016, pp. 94–97. doi:10.1109/REW.2016.030.

[30] A. Muyanja, P. I. Musasizi, C. Nassimbwa, S. S. Tickodri-Togboa, E. K. Kayihura, A. Ngabirano, Requirements engineering for the uganda police force crime records management system, in: 2013 21st IEEE International Requirements Engineering Conference (RE), 2013, pp. 30–307. doi:10.1109/RE.2013.6636734.

[31] T. Kuznecova, D. Rangelov, J. Knotter, Cold Case - Solved & Unsolved:, European Law Enforcement Research Bulletin (2023) 245–254. URL: https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/541.

[32] D. Babushkina, A. Votsis, Epistemo-ethical constraints on AI-human decision making for diagnostic purposes, Ethics Inf Technol 24 (2022) 22. doi:10.1007/s10676-022-09629-y.

[33] NATO, NATO - AJP-2.1 - ALLIED JOINT DOCTRINE FOR INTELLIGENCE PROCEDURES | GlobalSpec, 2016. URL: https://standards.globalspec.com/std/10019469/AJP-2.1.

[34] M. vanKeulen, Probabilistic Data Integration, in: A. Zomaya, J. Taheri, S. Sakr (Eds.), Encyclopedia of Big Data Technologies, Springer International Publishing, Cham, 2020, pp. 1–8. doi:10.1007/978-3-319-63962-8_18-2.