

A SYSTEMATIC LITERATURE REVIEW OF TRUST AND REPUTATION SYSTEMS IN
THE HIDDEN ECONOMY OF THE DARK WEB

by

MICHAEL MICHLOWSKI

B.S., George Mason University, 2009

M.S., The George Washington University, 2012

M.B.A., University of Massachusetts-Amherst, 2019

M.S., Georgia Institute of Technology, 2021

A Research Paper Submitted to the School of Computing Faculty of
Middle Georgia State University in
Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2026

A systematic literature review of trust and reputation systems in the hidden economy of the dark web

Michael Michlowski, *Middle Georgia State University*, michael.michlowski@mga.edu

Abstract

The dark web sustains a complex, hidden economy where illicit goods and services are exchanged amid anonymity, legal risk, and persistent uncertainty. In the absence of formal review and governance institutions, trust and reputation systems serve as essential governance mechanisms that enable market stability and repeated interaction among anonymous participants. The design of controls and verification mechanisms is a critical channel for close inspection and competitive advantage. Vendor reputation profiles, feedback and dispute platforms, escrow arrangements, and informal social norms are among the tools used to regulate behavior among market participants. Buyers expect multiple signals to indicate a vendor's legitimacy throughout a transaction. This paper presents a systematic literature review of trust and reputation systems operating within dark web marketplaces and related underground platforms. The findings contribute to a deeper understanding of how illicit online markets self-regulate and persist despite structural instability and external disruption.

Keywords: dark web, market trust systems, hidden economy, reputation mechanisms, online fraud

Introduction

The dark web is a decentralized platform where illicit goods and services are traded anonymously. This complex ecosystem comprises numerous online marketplaces where trust is critical to facilitating transactions between vendors and buyers (Jung et al., 2022). Unlike traditional e-commerce platforms, which often rely on third-party reviewers or buyer protection programs to establish trust, the dark web operates without such mechanisms, requiring buyers and vendors to develop their own trust-building methods. This has led to the development of informal, unique, and creative techniques, such as reputation systems, escrow platforms, and decentralized feedback solutions, designed to mitigate the risks associated with anonymity and fraud (Macanovic & Przepiorka, 2023). These mechanisms not only sustain the hidden economy but also offer critical insights into digital trust models relevant to legitimate decentralized systems.

Because these trust systems are central to dark web e-commerce, there remains a lack of comprehensive understanding of their effectiveness and role, including a systematic analysis of the mechanisms that sustain trust across multiple markets over time. Given the unpredictable lifespans of many dark web markets, driven by law enforcement actions or internal conflicts, understanding how trust is established, maintained, and monitored is critical to understanding overall market dynamics on the dark web (ElBahrawy et al., 2020). This understanding offers guidance for policy development, cybersecurity considerations, and future research on digital trust in decentralized environments. This research, through a comprehensive and systematic literature review, explores the various vendor trust mechanisms used on the dark web. The review focuses on identifying, categorizing, and evaluating trust mechanisms, their operational characteristics, and their influence on participant behavior.

This research will answer the following question:

RQ1: What themes emerge during a systematic literature review (SLR) of trust and reputation systems on the dark web?

Review of Literature

The dark web is a complex labyrinth of websites that host a variety of marketplaces selling illicit goods, such as drugs, weapons, stolen credentials, and hacking-related services (Kühn et al., 2024). Since the mid-2000s, dark web marketplaces have included well-known and documented examples such as The Silk Road and Alpha Bay (Gond, 2025). Primarily accessed via the The Onion Router (TOR) network, individuals navigate to these sites to obtain goods or services anonymously (Nazah et al., 2020). However, how buyers and sellers interact under the cloak of anonymity is critical to successful commerce and the continued operation of the dark web (Brinck et al., 2023). With a constantly changing landscape of dark web marketplaces, driven by law enforcement actions or simply by a loss of interest in running a marketplace, there is a need to establish and communicate confidence in products and services between buyers and sellers (Hayes et al., 2018).

Building trust and confidence on the dark web, however, faces numerous challenges and considerations. Certain attacks observed on the public Internet (i.e., “clearnet”) are also used on the dark web. For instance, phishing, a popular attack vector, is used on dark web marketplaces. As a result, there is a proliferation of cloned and illegitimate dark web marketplaces (Kaur & Randhawa, 2020). This creates an opportunity for bad actors to trick unsuspecting individuals into paying for non-existent items. It is therefore necessary to ensure that customers access legitimate markets (Wang et al., 2025). This requires proper implementation of site legitimacy confirmation to encourage customers and increase the likelihood of a successful two-party transaction (Geogoulas et al., 2021).

While anonymity is a core principle of the dark web, buyer payment transactions and shipping information ultimately require communication with the seller of a product or service. Until a history of transactions between buyer and seller is established, there is initial skepticism on both sides (Pace, 2016). However, by encouraging the use of encryption for every message, particularly Pretty Good Privacy (PGP), a marketplace vendor can protect sensitive information while still fulfilling their market obligation (Copeland et al., 2019). Additionally, to build marketplace confidence and establish a competitive advantage, a vendor can explicitly reference their security practices to increase trust with potential buyers. One example of buyer protection is securely deleting daily transaction records (Laferrriere & Decary-Hetu, 2021).

Traditional review mechanisms commonly found on legitimate markets are not always readily available on the dark web. From a buyer’s perspective, vendor confidence is an important factor in ensuring the successful and complete delivery of a product (Maras et al., 2023). A buyer places significant importance on reviewing a seller’s market profile and associated ratings from prior sales to gauge an initial level of confidence (Childs et al., 2021). Additionally, self-policing within a marketplace community is important, as there is no governing body or policymaking authority to provide oversight (Lund, 2019).

Methodology

This study used a systematic literature review, a critical component of purposeful academic research, to identify potential research gaps. This approach helps advance overall knowledge on an existing topic and creates opportunities for future research (Paul et al., 2023). Following established guidelines and procedures outlined by Maria Watson and Yu Xiao (2017) ensured a comprehensive, transparent, and replicable examination of existing research relevant to various research questions. Xiao and Watson’s (2019) process consisted of establishing a research inquiry, validating the review protocol, searching for literature, assessing inclusion criteria, assessing quality, extracting data, analyzing data, synthesizing data, and reporting the findings. Furthermore, based on Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) and guidance outlined by Mishra and Mishra (2023), a structured and logical assessment process was used for inclusion, quality, and associated data analysis. Figure 1 provides a graphical explanation of this process.

Searching the Literature

The following search string was used to identify research articles for potential inclusion in the study: “dark web” + vendor + trust + transaction + review + rating + operation. While this search string may be considered restrictive or introduce bias, it is important to recognize the niche topic of trust systems within the large body of dark web research papers. A granular focus is necessary to reduce noise in the search results. Google Scholar and the Georgia Library Learning Online (“GALILEO”) were used to search online academic databases with the search string listed above. Due to the rapidly evolving landscape of information technology, including the complex and dynamic nature of the dark web, the review included only articles published between 2019 and 2025. This search resulted in 268 articles for further review.

Inclusion Screening

A review of article abstracts was used to initially understand each article's general purpose and its relevance to dark web marketplaces. Additionally, the results and conclusion sections were reviewed for relevance and alignment with the overall research topic and the application research question. If applicable, testing procedures and approaches were evaluated for comprehensiveness (Affengruber et al., 2022). After this step, 112 articles were selected for further review.

Quality Assessment

Peer-reviewed, full-text articles were then used to assess quality. Quality considerations included a review of the paper title, scholarly approach, authoritative sources, and associated references (Baethge et al., 2019). Conference proceedings, non-peer-reviewed articles, and non-English articles were excluded at this step. 35 papers met the above quality assessment filters.

Data Analysis

Research articles were then categorized by themes and their relevance to the research question. Quantitative articles were reviewed for results and reporting methods (e.g., confidence intervals, ratios, or other statistically based measures) (Popenoe et al., 2021). Qualitative-based articles were reviewed for their interpretation methods (e.g., thematic analysis, case studies, or other qualitative methods).

Additionally, during this process, inductive coding in Microsoft Excel was used to organize the research into key themes to help address the research question associated with this research paper. During analysis, two recurring themes emerged. Papers were organized into two key themes, depending on whether they addressed specific vendor- or buyer-trust considerations or focused on side-wide trust characteristics.

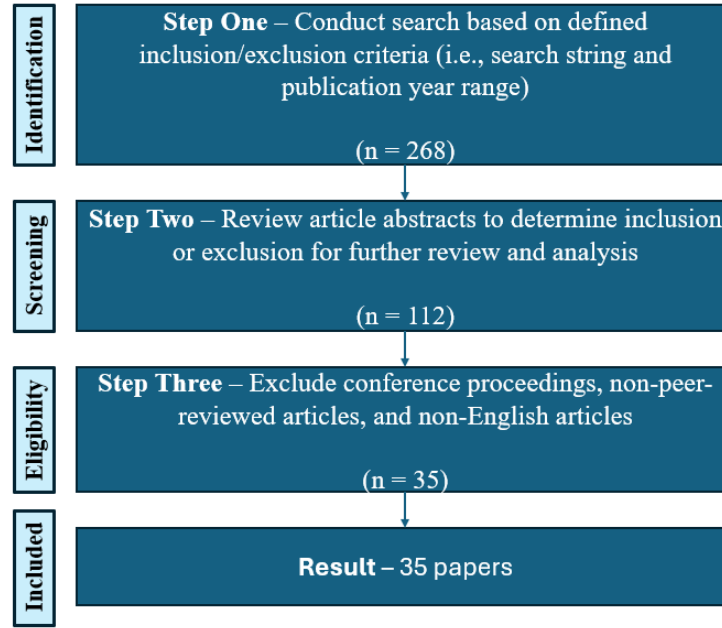


Figure 1: PRISMA Flow Diagram Structure

Results

The table below summarizes the key characteristics of the selected papers, including publication year, paper research methodology, and theme alignment. 54.3% of papers utilized quantitative research principles, 40.0% used qualitative research methods, and 5.7% used mixed methods. Many of the papers were published between 2022 to 2025.

Attribute		Count
Publication Year		
	2019	3
	2020	2
	2021	4
	2022	5
	2023	11
	2024	5
	2025	5
Research Methodology		
	Quantitative	19
	Qualitative	14
	Mixed Methods	2
Theme Category		
	Dark web marketplace sitewide trust	14
	Dark web vendor-specific trust signals	21

Table 1: Summary of Included Papers

Theme 1: Dark Web Marketplace Sitewide Trust

There is a consistent theme in how dark web marketplaces are structured. Regardless of which products are available for sale, many marketplaces follow a general approach to listing goods and services. This can even be as simple as being available only during specific times when dark web transactions are typically conducted (Tsuchiya & Hiramoto, 2020). Additional information on this theme is summarized in Table 2.

Connolly et al. (2023) evaluated marketplace sites to determine, in general, what goods and services are available for purchase on the dark web. This information informed the development of categories and groupings for organizational purposes. Overall, the categories are broad and not always granular (e.g., “guides”, “hacking”, and “passwords”). One exception, however, is when a marketplace targets a very specific customer. For instance, Copeland et al. (2019) assessed multiple weapon marketplaces and observed a catalog-style approach to showcasing weapons by category.

Georgoulas et al. (2021) observed two popular payment methods used to purchase on a marketplace. Bitcoin (BTC) remains a popular choice, while Monero (XMR) is increasingly accepted for its enhanced transaction privacy. Other forms of payment are also accepted, though less commonly. Other payment methods include Litecoin (LTC), Zcash (ZEC), and Ethereum (ETH). Jung et al. (2022) extended this finding by noting that payment methods that use an escrow service provide additional security.

General security mechanisms for dark web marketplaces are important. In a study by Wang et al. (2025), commonly observed practices include rate limiting, the Completely Automated Public Turing test (CAPTCHA), and waiting queues. These security features also help manage traffic and prevent site overload. In addition, it is important to develop a holistic perspective of the marketplace to increase a buyer’s confidence. One method of accomplishing this is to use other websites to verify a market’s legitimacy (Alharbi et al., 2021). Using either Clearnet or other dark web sites to vet a given marketplace helps build consensus that it is a good resource for purchasing a product.

Article Author(s)	Publication Year	Contribution
Alharbi, A., Faizan, M., Alosaimi, W., Alyami, H., Agrawal, A., Kumar, R., & Khan, R. A.	2021	Topology analysis of Clearnet and dark web interactions.
Connolly, K., Klempay, A., McCann, M., & Brenner, P.	2023	Developed a listing of various dark web market categories.
Copeland, C., Wallin, M., & Holt, T. J.	2019	Explored six dark web weapon-based marketplaces for marketplace characteristics.
Georgoulas, D., Pedersen, J. M., Falch, M., & Vasilomanolakis, E.	2021	Evaluated 41 marketplaces to gather information on vendor mechanisms and features.
Jung, B. R., Choi, K., & Lee, C. S.	2022	Assessed 148 dark web financial-based marketplaces for transaction-related characteristics.
Tsuchiya, Y., & Hiramoto, N.	2020	Determined when marketplace transactions typically occur.
Wang, Y., Arief, B., & Hernandez-Castro, J.	2025	Analyzed 12 marketplaces and their security features.

Table 2: Summary of Articles for Theme 1

Theme 2: Dark Web Marketplace Vendor Specific Trust Signals

Numerous dark web marketplaces gravitate towards commonly used trust mechanisms to build and maintain vendor and customer confidence. Regardless of site traffic or sophistication, many marketplaces follow similar practices when connecting buyers and sellers. Each method has a specific purpose, and a combination of these elements is important for a comprehensive profile of a buyer or seller. Even specific details regarding shipment practices and the level of packaging sophistication come into play (Kamphausen & Werse, 2019). Additional information on this theme is summarized in Table 3.

Maras et al. (2023) observed specific characteristics increasing buyer confidence when shopping for products. These include a comprehensive vendor profile with affiliations, the entire order process, a biography, and a secure communication channel. Regarding a vendor biography, explaining the overall motivation for selling a product and why it can even have a positive sales impact (Martin et al., 2019). Even communicating the quantity available for sale provides a perspective of operational size. Additionally, having a feedback system front and center allows customers to write and read detailed narratives about the product and transaction.

Seeing a vendor and its associated products across multiple marketplace sites demonstrates to a buyer the vendor's potential size and sophistication. It also shows the vendor has passed multiple marketplace validation checks (Li et al., 2021). Being listed on multiple marketplace sites also allows for a potential exit scam to be more quickly detected and communicated between dark net sites (Norbutas et al., 2020).

The protection of personal and purchase data is a critical concern for buyers (Kiss & Szigeti, 2023). Sellers should have a plan for how information is captured and deleted upon completion of the transaction. An additional benefit, although significantly slower, is the availability of offline payment methods, such as cash. A vendor's overall helpfulness demonstrates the level of customer service.

Laferrière & Décary-Héту (2021) extended the analysis of trust signals and noted that certain vendor narratives help buyers connect more effectively. Providing price comparisons, refund policies, and external reviews helps give a holistic picture of a given vendor. At the most basic level, including product pictures provides a visual indication of product quality.

Article Author(s)	Publication Year	Contribution
Kamphausen, G., & Werse, B.	2019	Evaluation of shipping methods for marketplace transactions.
Kiss, T., Szigeti, A.	2023	Survey of important trust factors.
Laferrière, D., & Décary-Héту, D.	2021	Data scraping of vendor characteristics.
Li, Z., Du, X., Liao, X., Jiang, X., & Champagne-Langabeer, T.	2021	Assessment of trends across multiple marketplace sites.
Maras, M., Arsovska, J., Wandt, A. S., & Logie, K.	2023	Establishment of a trustworthiness index.
Martin, J., Munksgaard, R., Coomber, R., Demant, J., & Barratt, M. J.	2019	Interviews with vendors to understand motivations.
Norbutas, L., Ruiters, S., & Corten, R.	2020	Analysis of reputation systems across multiple marketplace sites.

Table 3: Summary of Articles for Theme 2

Discussion

A review of the literature reveals two clear themes about overall trust in dark web marketplaces, regardless of what is sold (i.e., illicit goods or illegal activities). Each theme highlights key security concerns to ensure a market transaction goes smoothly. Both themes support each other and strengthen trust during interactions between buyers and vendors.

Theme one emphasizes sitewide security features that serve as the marketplace's overall boundary. These are the initial building blocks of a large-scale trust model between vendors and buyers. This is similar to a physical store, with security measures such as cameras and alarm systems. Vendors likely rely heavily on these sitewide security features to operate their businesses, adding more specific, individual security controls on top of an already established and reputable marketplace website. Wang et al. (2025) confirm this through certain site-specific protection features, while Alharbi et al. (2021) layer on top of site-security features by using other resources to verify legitimacy.

The second theme becomes more specific, focusing on individual seller and vendor traits, such as what makes them stand out from competitors. These security considerations address the specific nuances of a particular marketplace and its related product. For example, illicit goods that require physical delivery will need extra trust-verification steps compared to digital delivery, such as stolen credentials. Kamphausen & Werse (2019) elaborate on the need to carefully address and explain the packaging process. Additionally, Laferrière & Décary-Héту (2021) suggest that a comprehensive vendor profile can align with expectations, depending on the product type.

This research and the associated literature review indicate alignment with general, well-accepted security principles for conducting transactions on the dark web. Vendor and buyer review mechanisms, encryption, and monitoring are key tenets of a well-rounded, secure, and trustworthy platform. The research also indicates that good marketing is an important layer for overall success.

Conclusion

Dark web marketplaces remain a fascinating area to study how illegal transactions succeed. By adopting multiple security measures from the surface web, both vendors and buyers continue to customize their systems in response to changing conditions and real-world factors. Just like prisoners who get creative in avoiding rules, dark web users are clever in developing their own ecosystems. However, this can all end suddenly due to law enforcement action or a site owner deciding to shut down and make a quick buck.

The literature review emphasizes common elements for transactions, such as defending against site-wide availability attacks (like DDoS), securing communication channels, and informing the community about the legitimacy of vendors or buyers. All are crucial parts of a system operating under questionable conditions. If one fails or falls short, others may also fail or become severely compromised.

Implications and Recommendations

Researching and investigating dark web marketplaces and related transactions can benefit many others, such as law enforcement, groups monitoring illegal trade, and researchers interested in the topic. Learning from these efforts can certainly help legitimate businesses identify potential security gaps in their marketplace models and make necessary adjustments. Dark web market transactions and the associated ecosystem may also reveal specific efficiencies that are not yet realized on the clear web.

There is also potential for further research in this area. One suggestion is to develop and expand a conceptual framework to better evaluate and measure the specific security mechanisms used by vendors and buyers. Additionally, work can be done to investigate and identify any conflicting findings and explore why such differences may exist, either due to specific marketplace conditions (i.e., product type/mix) or historical considerations.

Finally, future research can explore potential search bias when finding literature relevant to the research topic. Many research papers cover various aspects of the dark web, and it is important to include all relevant sources that mention a marketplace. One suggestion is to expand the scope by year and keywords.

References

- Affengruber, L., Dobrescu, A., Persad, E., Klerings, I., Wagner, G., Sommer, I., & Gartlehner, G. (2022). Characteristics and recovery methods of studies falsely excluded during literature screening—a systematic review. *Systematic Reviews*, 11(1), 236. <https://doi.org/10.1186/s13643-022-02109-w>
- Alharbi, A., Faizan, M., Alosaimi, W., Alyami, H., Agrawal, A., Kumar, R., & Khan, R. A. (2021). Exploring the topological properties of the TOR dark web. *IEEE Access*, 9, 21746–21758. <https://doi.org/10.1109/access.2021.3055532>
- Baethge, C., Goldbeck-Wood, S., & Mertens, S. (2019). SANRA—a scale for the quality assessment of narrative review articles. *Research Integrity and Peer Review*, 4(1), 5. <https://doi.org/10.1186/s41073-019-0064-8>
- Brinck, J., Nodeland, B., & Belshaw, S. (2023). The “yelp-ification” of the dark web: an exploration of the use of consumer feedback in dark web markets. *Journal of Contemporary Criminal Justice*, 39(2), 185–200. <https://doi.org/10.1177/10439862231157519>
- Childs, A., Bull, M., & Coomber, R. (2021). Beyond the dark web: navigating the risks of cannabis supply over the surface web. *Drugs Education Prevention and Policy*, 29(4), 403–414. <https://doi.org/10.1080/09687637.2021.1916439>
- Connolly, K., Klempay, A., McCann, M., & Brenner, P. (2023). Dark web marketplaces: data for collaborative threat intelligence. *Digital Threats Research and Practice*, 4(4), 49, 1–12. <https://doi.org/10.1145/3615666>
- Copeland, C., Wallin, M., & Holt, T. J. (2019). Assessing the practices and products of darkweb firearm vendors. *Deviant Behavior*, 41(8), 949–968. <https://doi.org/10.1080/01639625.2019.1596465>
- ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., & Baronchelli, A. (2020). Collective dynamics of dark web marketplaces. *Scientific Reports*, 10(1), 18827. <https://doi.org/10.1038/s41598-020-74416-y>
- Georgoulas, D., Pedersen, J. M., Falch, M., & Vasilomanolakis, E. (2021). A qualitative mapping of darkweb marketplaces. *2021 APWG Symposium on Electronic Crime Research (eCrime)*. <https://doi.org/10.1109/ecrime54498.2021.9738766>
- Gond, A. K. (2025). Hidden side of the Internet: Between crime and freedom on the Dark-Web. *Journal of Communication and Management*, 4(03), 55–61. <https://doi.org/10.58966/jcm2025436>

- Hayes, D., Cappa, F., & Cardon, J. (2018). A framework for more effective dark web marketplace investigations. *Information*, 9(8), 186. <https://doi.org/10.3390/info9080186>
- Jung, B., Choi, K., & Lee, C. (2022). Dynamics of dark web financial marketplaces: An exploratory study of underground fraud and scam business. *International Journal of Cybersecurity Intelligence and Cybercrime*, 5(2), 4–24. <https://doi.org/10.52306/xmhn2624>
- Kamphausen, G., & Werse, B. (2019). Digital figurations in the online trade of illicit drugs: A qualitative content analysis of darknet forums. *International Journal of Drug Policy*, 73, 281–287. <https://doi.org/10.1016/j.drugpo.2019.04.011>
- Kaur, S., & Randhawa, S. (2020). Dark web: a web of crimes. *Wireless Personal Communications*, 112(4), 2131–2158. <https://doi.org/10.1007/s11277-020-07143-2>
- Kiss, T., & Szigeti, Á. (2023). Ranking trust factors affecting risk perception in illicit drug purchase on the Darknet: a Large-Scale Survey study in Hungary. *European Journal on Criminal Policy and Research*, 31(1), 61–76. <https://doi.org/10.1007/s10610-023-09545-x>
- Kühn, P., Wittorf, K., & Reuter, C. (2024). Navigating the Shadows: Manual and Semi-Automated Evaluation of the Dark Web for Cyber Threat intelligence. *IEEE Access*, 12, 118903–118922. <https://doi.org/10.1109/access.2024.3448247>
- Laferrière, D., & Décary-Héту, D. (2022). Examining the uncharted dark web: trust signalling on single vendor shops. *Deviant Behavior*, 44(1), 37–56. <https://doi.org/10.1080/01639625.2021.2011479>
- Li, Z., Du, X., Liao, X., Jiang, X., & Champagne-Langabeer, T. (2021). Demystifying the dark web opioid trade: content analysis on anonymous market listings and forum posts. *Journal of Medical Internet Research*, 23(2), e24486. <https://doi.org/10.2196/24486>
- Lund, B. (2019). The dark web for all! Why this polarizing "crime haven" might just be our best chance to preserve our right to privacy and intellectual freedom. *Journal of Information Ethics*, 28(2), 109–116. <https://www.proquest.com/scholarly-journals/dark-web-all-why-this-polarizing-crime-haven/docview/2317012446/se-2>
- Macanovic, A., & Przepiorka, W. (2023). The moral embeddedness of cryptomarkets: text mining feedback on economic exchanges on the dark web. *Socio-Economic Review*, 22(4), 1705–1732. <https://doi.org/10.1093/ser/mwad069>
- Maras, M., Arsovska, J., Wandt, A. S., & Logie, K. (2023). Keeping pace with the evolution of illicit darknet fentanyl markets: using a mixed methods approach to identify trust signals and develop a vendor trustworthiness index. *Journal of Contemporary Criminal Justice*, 39(2), 276–297. <https://doi.org/10.1177/10439862231159530>
- Martin, J., Munksgaard, R., Coomber, R., Demant, J., & Barratt, M. J. (2019). Selling drugs on Darkweb Cryptomarkets: Differentiated pathways, risks and rewards. *The British Journal of Criminology*, 60(3), 559–578. <https://doi.org/10.1093/bjc/azz075>
- Mishra, V., & Monu Pandey Mishra. (2023). PRISMA for Review of Management Literature – Method, Merits, and Limitations – An Academic Review. *Emerald Publishing Limited EBooks*, 2, 125–136. <https://doi.org/10.1108/s2754-586520230000002007>

- Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of dark web threat analysis and detection: a systematic approach. *IEEE Access*, 8, 171796–171819. <https://doi.org/10.1109/access.2020.3024198>
- Norbutas, L., Ruiter, S., & Corten, R. (2020). Believe it when you see it: dyadic embeddedness and reputation effects on trust in cryptomarkets for illegal drugs. *Social Networks*, 63, 150–161. <https://doi.org/10.1016/j.socnet.2020.07.003>
- Pace, J. (2016). Exchange relations on the dark web. *Critical Studies in Media Communication*, 34(1), 1–13. <https://doi.org/10.1080/15295036.2016.1243249>
- Paul, J., Khatri, P., & Duggal, H. K. (2023). Frameworks for developing impactful systematic literature reviews and theory building: What, Why and How? *Journal of Decision System*, 33(4), 537–550. <https://doi.org/10.1080/12460125.2023.2197700>
- Popenoe, R., Langius-Eklöf, A., Stenwall, E., & Jervaeus, A. (2021). A practical guide to data analysis in general literature reviews. *Nordic Journal of Nursing Research*, 41(4), 175–186. <https://doi.org/10.1177/2057158521991949>
- Tsuchiya, Y., & Hiramoto, N. (2020). Dark web in the dark: Investigating when transactions take place on cryptomarkets. *Forensic Science International Digital Investigation*, 36, 301093. <https://doi.org/10.1016/j.fsidi.2020.301093>
- Wang, Y., Arief, B., & Hernandez-Castro, J. (2025). Secure in the dark? An in-depth analysis of dark web markets security. *International Journal of Information Security*, 24(3), 107. <https://doi.org/10.1007/s10207-025-01015-1>
- Xiao, Y., & Watson, M. (2017). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research*, 39(1), 93–112. <https://doi.org/10.1177/0739456x17723971>