SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 5078-5090
Open Access. Online & Print

DOI: 10.5281/zenodo.19113531

THE ROLE OF DARKNET IN FACILITATING ORGANISED CRIME: LEGAL AND CRIMINOLOGICAL PERSPECTIVE"

Dalia Kadry Ahmed Abdelaziz[1]

[1]Assistant Professor of criminal law, Prince Sultan Univesity
Saudi Arabia- Riyadh, https://orcid.org/0000-0002-7616-5827

Received: 06/02/2026
Accepted: 05/03/2026

Corresponding Author: Dalia Kadry Ahmed Abdelaziz
(dkadry@psu.edu.sa)

ABSTRACT

The Darknet has become a critical facilitator of organized crime by offering unique, anonymous access to a variety of illegal activities ranging from drug trafficking to cybercrime. This paper delves more into the murky waters of the Darknet in organized crime from legal, as well as at the level of criminology, and delves into exactly how the system that is Darknet and the practices it performs encourage even more criminal acts and further hinders law enforcement. One major challenge is existing jurisdictional ambiguities, and loopholes in the current laws that are not equipped to handle the current criminal methods. If the author's views are proved correct, successful methods of fighting organized crime on the network should include as well as a legal reform and international cooperation. This literature survey is also a tool.

KEYWORDS: Darknet, Organized Crime, Cybercrime, Law Enforcement, Digital Anonymity.

1. INTRODUCTION

The Darknet is a specialized segment of the internet accessible exclusively through proprietary applications such as Tor, which provide users with advanced encryption and preserve their anonymity. Unlike the surface web — which is openly indexed and publicly accessible — and the deep web, where a vast amount of legitimate yet hidden data resides, the Darknet is explicitly designed to keep users and their activities largely beyond the reach of conventional surveillance techniques (Luong, 2024). This distinct and largely unregulated environment has facilitated a wide range of illicit activities, including drug trafficking, human exploitation, and cybercrime (Bertola, 2020).

Particularly alarming is the Darknet's facilitation of exploitation targeting vulnerable populations, especially women and children, who are frequently victims of trafficking and abuse through underground commercial exchanges (Bertola, 2020). Such crimes inflict profound and lasting harm on public safety and undermine long-established social norms intended to protect against such abuses. The transnational nature of the Darknet introduces both legal and technical complexities, including data anonymization, jurisdictional fragmentation, and the intricate organization of decentralized criminal networks, all of which severely hinder law enforcement efforts (Hartmann, 2025). Consequently, traditional investigative tactics often fail to identify perpetrators and secure prosecutable evidence under these circumstances.

From a criminological perspective, the Darknet challenges conventional frameworks that focus on hierarchical and geographically bounded criminal organizations. Instead, it fosters more fluid and decentralized networks sustained by virtual trust mechanisms, such as reputation-based systems, representing a paradigm shift in the organizational governance of crime (Bancroft, 2020). Meanwhile, legal frameworks have lagged considerably behind technological advances, creating exploitable gaps that organized crime groups readily capitalize on. The fragmentation of legal jurisdictions further exacerbates these issues, underscoring the urgent need for enhanced international cooperation and harmonized legal standards (European Union, 2008).

Effectively combating the organized crime empowered by the Darknet requires an interdisciplinary approach integrating legal reform, criminological theory, and technological innovation. Increasing awareness of the unique challenges posed by anonymous digital environments will enable law enforcement agencies to develop more proactive and effective prevention and intervention strategies (Jardine, 2021).

This paper seeks to contribute to the scholarly understanding of the Darknet's facilitative role in organized crime by examining its impact through legal and criminological lenses. It highlights the critical necessity of radical legal reforms alongside multifaceted and strategic responses capable of curbing the growth of illicit activities and fostering a safer, more resilient society in the digital age

2. EXPANDED LITERATURE REVIEW: THE ROLE OF DARKNET IN FACILITATING ORGANIZED CRIME—LEGAL AND CRIMINOLOGICAL PERSPECTIVE

Building upon the foundational insights presented in the introduction regarding the Darknet's complex nature and its facilitative role in organized crime, this section undertakes an expanded review of the existing legal and criminological literature. By examining diverse perspectives, it aims to illuminate the duality of the Darknet as both a protector of privacy and a hub of illicit activities, highlighting the challenges it poses to traditional justice systems.

it is important to recognize that the darknet is really a far more complex computer space and as such can be perceived as a place where it is perfectly legitimate — protecting the privacy of journalists and political dissidents while also being a source for many illegal activities that are organized behind a screen on the darknet. Its distinct form is anonymous and is an architectonic one that gives a decentralized structure to such a network which confounds the ability of law enforcement agencies to investigate and prosecute criminal offenders (Luong, 2024), which explains this dual nature. It is essential that we consider a wide range of viewpoints to understand the Darknet's broad-based consequences for society and justice systems. The darknet allows an ecosystem free of the risk of being subjected to criminal investigation and crime. Darknet anonymity fosters an environment where crime is not only a crime, it is a way of life. Users use the same digital social infrastructure to preserve these underground marketplaces, and users also leverage an ecosystem of trust intermediaries--reputation systems, encrypted communications, etc.--to underpin these nefarious activities, all cloaked in secrecy (Bancroft, 2020). These dynamics challenge standard criminological thinking because the logic maintains that it is territorial, hierarchical control of crime which is more pertinent and hence theoretical frameworks need to develop in regard to the

dynamic and online-offline dualism of darknet criminology (Pertola, 2020). In addition to this, a need for studies pertaining to the darknet's association with mobile apps is evident, along with its privacy and security implications being proven with respect to the varying risks to user data (Tovino, 2020; Harrison, 2016).

2.1 Economic Implications

The darknet and its evolution in organized crime is understood in an economic analysis. Crypto markets are organised economic ecosystems where large-scale, anonymous illicit goods transactions are organized and in this way drug, weapon, and other illegal goods trade transmissions occurring globally on a global and large scale. Dutta (2025) describes how these markets transform established networks of illicit drug use via governance mechanisms and cryptocurrencies as new frontiers of governance and a means of circumventing formal financial mechanisms and global crimes' economics around the world—and the world of crime and economic structure under which they operate, that is the form of capital theft. This is akin to insider trading dynamics whereby criminal groups are able to use a loose regulatory vacuum that is very much like insider trading (Mc and Mtenzi, 2011; Ditta, 2017).

2.2. Legal Framework and Difficulties

The darknet illustrates the limitations of existing laws, from a legal perspective. These are fragmented jurisdictions, slow legal reactions and weak international coordination, inhibiting effective reaction to darknet wrongdoing (Hartmann, 2025; European Union, 2008). Scholars like Khobbi et al. (2022) call for serious reforms that will enhance their law enforcement capacity while safeguarding human rights. Tennant (2021) explains how the problems of consistent international conventions in terms of enforcing transnational organized crime law and the darknet compound the problem. It all got worse when networks were flourishing that enabled minors to freely access data or services like medical apps and digital devices to link to the darknet. Recent examples have been presented with respect to sex trafficking, sexual abuse and disseminating child sexual abuse material (Gannon et al., 2023), highlighting the difficulties of coping with current legal paradigms in a world where new modes of digital activity are emerging. Finally, legal measures like those on privacy, data protection and data protection regarding mobile health and apps can inform us of what laws are required for addressing similar difficulties for darknet activities (Tovino, 2020). Kirk et al.'s (2012) discussion of inclusive policing models points out some of the positive and problematic aspects of using these measures for local cooperation to enhance policing in a complex setting.

2.3. Trust Dynamics in Darknet Communities

Trust mechanisms in darknet markets are fundamental to maintaining operations functionality. Although these efforts are purely criminal, anonymous users still rely on reputation systems, dispute resolution, and encrypted communication for increased reliability (Bancroft, 2020). Incorporating micro-case studies into these systems would enhance our understanding of how crime networks establish cohesion within virtual space.

2.4 Future Research directions

Reflections: Looking towards the future, I believe it would be helpful to explore how emerging trends in a flourishing darknet, including the identification or even development of new methods of illicit trade and technology employed by criminals, may have developed in similar areas. In fact, comparisons between international legal responses and enforcement strategies will help to identify best practice and deficiencies of existing international governance mechanisms (Ovsianiuk et al., 2025). Moreover, to counter the complexities of the darknet's criminal landscape, these dynamics will necessitate interdisciplinary efforts that integrate legal education with criminology, economics and technology to come up with the best adaptive solutions (Wang et al., 2021).

3. THEORETICAL FRAMEWORK

Drawing from the diverse scholarship discussed, this paper now turns to a theoretical examination that integrates criminological theories and technological frameworks. This interdisciplinary lens is critical to comprehensively conceptualize how the Darknet facilitates organized criminal behaviours

This study's theoretical lens in this study is designed to understand the intricacies of the Darknet and, thus, organized crime. The combination of criminological research, academic and research on digital technology, legal practices, criminological studies, economics and economics lays a multi-pronged groundwork to reach a theoretical lens on crime utilizing the Darknet, in particular understanding the function of its operations in supporting organized crime. Especially, the Darknet is one of the most helpful mechanisms in conceptualising black market activity in organized

crime and can be explored as part of this. It expands on a range of theories and is influenced by new literature which identifies the ecology of criminal behaviour in this space.

3.1 Criminological Theories

Social Learning Theory Learning criminal behaviours becomes learned through interrelation and observation in a cultural context. Within the Darknet environment, users exist within a virtual subculture that justifies criminal commerce and tech misuse without any constraint. Leukfeldt and Holt (2019) suggested that trust systems in these markets, including reputation systems, offer an 'education environment" that can be conducive to drug trafficking and other criminal behaviours. These exchanges can significantly affect new users who continue to replicate such nefarious behaviours through their online journeys. Moreover, investigations of organizational in the context of cybercrime in recent years have shown that the subcultures of Darkeners engage in crime behaviour, suggesting that such subcultures may practice crimes at a global scale through their digital socialization. That is to say, it is clear that the classical model needs reforming to incorporate lessons from cyber sociology and economics of interaction. Crime is suspected in Routine Activity Theory as motivated offenders, target groups, and limited capable guardians in the public working together. The Darknet is where motivated offenders have access to potential usable targets--those individuals searching for black market products--that might escape or evade police control, although these venues are almost always anonymous (Moore & Clayton, 2015). This theory discusses how the environment of the Darknet contributes to organized crime on environmental scales.

3.2. Technological Frameworks

Technology to Organising Crime Technology plays an important part in the emergence of criminal organizations and we should not go overboard. Anonymization technologies such as Tor and cryptocurrencies are leading to scenarios which make it extremely difficult to carry out law enforcement. The development of Darknet technologies does not seem to lie in the hands of some individuals. Jardine et al. (2020) investigate the Tor network and find that although the internet network allows freedom of actions and interpretation, it also creates an abuse of that freedom, particularly in areas with poorly enforced internet privacy laws. The phenomenon illustrates both, how a technical infrastructure allows for criminal activity, whilst also raising key issues of digital anonymity governance and public policy. Additionally, Goonetilleke et al. (2023) identify major operational features of major darknet markets focusing on governance mechanisms — e.g. escrow services and feedback mechanisms — which provide participants with confidence in the platform while also reducing its control complexity. Hence, the dual character of these technologies mirrors the frequently complex relationship of privacy and criminality, as Dittus (2017) demonstrates through emerging illicit supply chains in drug markets (Hiramoto & Tsuchiya, 2022; Dittus, 2017). By understanding the logic and function of the darknet, you are able to do better to understand the market and the economic side to that game, specifically the cryptomarkets, and the role of these elements in the international crime and drugs scene. Bertola (2020) argues that darknet marketplaces alter the social networks that influence the wider drug sphere which then evolve into intricately complex markets driven by the logic of supply and demand and in turn influencing drug use generally. They're for the market, which connects buyers and sellers and sets up transactional networks that circumvent conventional control structures. The nature of cryptocurrencies on the Darknet is that its use is based on the decentralized nature of these transactions that criminals use to create crime, consequently this is a legal issue on the Darknet but unlike a society on other platforms. Cryptocurrencies provide the opportunity for cross-border transactions but they also hinder it for law enforcement to monitor the money related to illicit finances—showing that organized crime is changing in response to new technologies (Kethineni and Cao, 2019). Further, Weitz et al. (2025), link between economics and drug procurement patterns from different regions is another perspective on determining what the legal frameworks and economic stimulus in each region has had on the effectiveness of crime prevention approaches; laws that create barriers toward crime detection and recovery (Dhali et al., 2023)

3.3. Legal Frameworks and Challenges

Given laws that often lag behind the technological progression in the case of the rise of the Darknet and also create the complexity that is driving criminal enterprises to thrive on the darknet, the data-driven approaches to address the rise of organized crime are among its strongest challenge to legal systems. The jurisdictional legal terrain is fragmented and challenging to prosecute even where it connects

several legal jurisdictions (Dondjio, 2023). The EU's 2008 Framework Decision on Combating Organized Crime promotes this type of cooperation but the difficulty of the Darknet indicates that transnational crime requires different approach (Tzanetakis & Marx, 2023). Protasyevich and Skryabikova (2021) have observed the need for integrated identification of the "darknet" with criminalistics, which is imperative. An understanding of laws may serve as a foundation for effective law enforcement practices aimed at organized crime. Shevchuk and Voluiko (2025), in their study about organized crime's exploitation of the legal system, reveal how it can serve as a strong catalyst on shortcomings in legislation and improvement agenda (Bakken et al., 2017). 4. Strategies and Recommendations for Combating Organized Crime on the Darknet.

3.4. Strategies And Recommendations For Combating Organized Crime On The Darknet

For this to be successfully fought against criminal activity in the darknet they are going to have to be implemented. This implies the incorporation of legal, technical, educational and collaborative structures. These challenges brought about by the culture of the Darknet can be responded to through the following strategies through improved law, technical advances, training programs etc.

3.5. Enhancing National and International Legal Frameworks

It is essential that the legal architecture of countries will evolve and shift quickly with these quickly evolving technologies. No legislations need to be reactive; they need to be proactive. The law will have to be ready, and have the technical capacity to grapple with the intricacies of digital crime. Scholars stress the importance of international cooperation to address geographic divides and to develop treaties and universal standards (Jardine, 2021; Bertola, 2020). International legal standards would make extradition and enforcement mechanisms seamless across borders, because they will pose a greater obstacle to criminals in countries as potential suspects, who often have greater resistance to exploiting loopholes in the law with which they are connected in fragmented jurisdictions. More so, we must work at distinguishing between the legality and organized crime in the context of cryptocurrency. As (Tung, 2021) observes, the growing incorporation of electronic currencies into crime, hence, makes it necessary to establish stringent laws that can specifically concern financial technologies associated with organized crime (Tung, 2021& Achek et al., 2026).

3.6. Use advanced technologies for investigation and enforcement

Leveraging technology to investigate and enforce the use of new types of research and application of latest tech tools for investigation and policy, they become all the more effective. Big data analytics, artificial intelligence, machine learning and big data analysis and big data artificial intelligence technologies are excellent for enhancing law enforcement. With such technologies at their fingertips, agencies will be able to more easily discern trends and monitor illegal activities and crime activities with these tools, making it easier to locate trends in crime data. Specialized blockchain analysis tools are very high for researching the suspected illicit cryptocurrency flows, which are often used in the Darknet underworld (Jardine, 2021). Techniques such as approaches described by (Oosthoek et al., 2023), for instance, can be used to identify and measure illicit income and are key to cracking down on organized crime networks operating under the guise of anonymity (Oosthoek et al., 2023). AI also makes possible the identification and detection of cybercrime, but also the early prediction of future threats possible through it. In this sense AI detection for new types of cybercrime is to monitor the patterns in these networks (El-Kady, 2024). So there is promise in employing and embracing such technological development, that investigation and prosecution would be more productive.

3.7. Raising the Police Force's Capacity

There is a critical need for law enforcement officers to be able to capably handle cybercrime cases. The officers require continuous training and development in order to become proficient in addressing the challenges posed by Darknet activity (Bertola, 2020). This is how dedicated cybercrime units in law enforcement can help in the reduction of such resources and in the establishment of an expertise in combating such crime. In addition, it is described by (Gundur et al., 2021), the establishment of partnerships with academic institutions can provide access to research and trends in crime prevention-related fields (Gundur et al., 2021) that allows us to gain access to the research and current trends that is applicable to preventing crime and to be involved in this area, thus helping in criminal activities and this will be able to make law enforcement more effectively in the pursuit of crime prevention (Bright, 2024).

3.8. Awareness and Education

There is a need for great public interest public campaigns to keep a lid on such risks based on social and social safety risks in an increase of Darknet-based crime. Public awareness raises awareness of suspicious activity in the communities so they have better awareness of those activities and can report it. In addition, an important part of this is giving up that information security and privacy protection training to digital participants. Adopting measures like this would not only cut down the risk factors but also can foster a culture of vigilance and proactivity against digital assault that is proactive (Bertola, 2020). Collaboration between industry and industry-led research organizations could create a network of academic resources or sites for individuals to learn about the dangers involved with using the Darknet (Kaushik, 2022).

3.9. Partnership with Private Sector and Research Institutions

The partnership with Private Organizations and Research Institutions can be a viable means of combating organized crime in the Darknet. In collaboration with technology and internet companies, law enforcement can improve its surveillance and reporting on crimes emerging in cyberspace (Jardine, 2021). Moreover, promoting academic research such as blockchain- and cryptocurrency-transaction analysis of darknet activities can provide a fertile ground for academic insight into the darknet world (Dearden and Tucker, 2023) (Dearden & Tucker, 2023); such studies can help enhance our understanding of digital organized crime and new potential countermeasures to policing initiatives. Furthermore, agencies are called on to collaborate with stakeholders in the field of cybersecurity as well to be equipped to build a broad approach for addressing darknet crime.

4. CHALLENGES ON THE NEAR FUTURE IN COMBATING ORGANIZED CRIME ON THE DARKNET

Building on the strategies and recommendations outlined earlier, it is crucial to recognize that the rapid evolution of technology and criminal methods continuously reshapes the landscape of organized crime on the Darknet. Consequently, law enforcement and policymakers must anticipate emerging challenges and adapt their approaches accordingly.

Data is being collected from as far back as October 2023. The following section explores how new technologies (for better and worse) may affect organised crime, and highlights future legal and ethical issues. The chapter also addresses the necessity for fresh thinking and adaptability as a means of combatting organized crime on the Darknet.

4.1. The Continuing Development of Technologies

Advanced technologies in the form of artificial intelligence (AI), quantum computing and cryptographic techniques have a direct impact on organized crime operations in the Darknet. AI also expedites more advanced cyberattacks by automating vulnerability finding and attack management tasks. Quantum computing comes with some danger and an opportunity: It may also empower law enforcement to better analyze multitudinous databases and coordinate counter-cyber attacks with proactive crime (Wang et al., 2024) though not always with immediate results. Additionally, new encryption techniques present a problem for law enforcement agencies to monitor illegal situations. Regulatory bodies and law enforcement agencies must respond to these emerging technologies in the near future (Ceylan & Çetinkaya, 2019) and adapt their strategies and tools accordingly. A fundamental importance of this study is the understanding of the dynamics of how these emerging technologies work and what they may mean for both the proactive defence efforts and law enforcement responses. As stated by (Adel & Norouzifard, 2024), this has led to increased emphasis on the weaponization of cybercrimes with a growing need for deterrent measures against technologically advanced crime (Adel & Norouzifard, 2024).

4.2. Rise in New Crime Trends

New and more relevant patterns of crime emerge due to technological advances. The evolution of AI-powered cyberattacks poses an important concern, allowing attackers access to AI tools for more precise targeting and attack execution. Additionally, the prevalence of smart devices opened up additional avenue for crime, presenting some points of entry for cybercriminals to take advantage of interconnected environments (Javed et al., 2021). The rise of digital financial currencies — including non-fungible tokens (NFTs) and decentralized finance (DeFi) — further complicates cybercrime. However, this not only makes legitimate users a lucrative target, but also provides formal legal and organized crime methods to exploit unregulated financial systems (Khan et al.,

2024). The evolution in the dynamics of organized crime groups is changing also (Franata & Santiago, 2022) as offenders will increasingly move between platforms and adapt with new technologies; therefore, it will be critical for law enforcement to monitor these trends. Exploring the nature of offenders who engage with emerging digital financial technologies is important for understanding new methods in illicit trade and assisting law enforcement (El-Kady, 2024).

4.3. Legal and Ethical Challenges

Government efforts to regulate and monitor the Darknet have been ramping up, and the challenge is only growing, legal and ethically, at the intersection of privacy and human rights. There is a need to balance these new forms of increased surveillance with those that protect rights and freedoms as individuals. This balance is particularly critical for any discussion of surveillance and marginalized populations and wider ethics of invasive technologies: Buszko (2020). As they try to grapple with the rapidly evolving realities of organized crime, laws and rules will be heavily challenged to the best of their ability, as will the need to avoid placing citizens in harm's way in the way they want to be regulated. A conversation that addresses privacy concerns must refer to international standards for human rights, and the standards that underpin regulations should follow them (Abdulrauf, 2018). The study of conditional cyber-deterrence for police crackdowns on the Darknet implies a persistent requirement to carefully evaluate legal and ethical practices (Décary-Hêtu et al., 2023)

4.4. The Requirement For Innovation And Flexibility

Against these new threats, innovation for, and flexibility of legal structures, enforcement mechanisms and technological tools is indispensable. Periodic updating of laws relevant to cybercrime is necessary to ensure the digital world keeps pace with organized crime activity. Policymakers should employ nimble approaches to catch modern day technology, so that the law is current and working. In addition, promoting the cooperation of the government, technology industry, and research institutes can generate important views and creative thinking to the public safety, and effectiveness with respect to law enforcement (Eskens, 2020, Ven & Koenraadt, 2017). These cross-sector collaborations could result in a generation of frameworks that employ AI and emerging technologies to pre-emptively prevent and respond to crime.

4.5. Future Research Issues: Holistic Approaches to Organized Crime with the Darknet

With an increased emphasis on the Darknet, as a nexus of organized crime, it is clear that complex and robust research paradigms are an important tool in managing criminal operations, law enforcement, and criminological insight in this particular field. Development of the comprehensive lifecycle models that can evaluate the activities of the criminal networks operating on the Darknet should focus on future research and proposed intervention strategies.

4.6. Interdisciplinary Research Collaborations

Combining criminology, cybersecurity, legal and economic research can guide holistic strategies to prevent organized crime taking place in the Darknet. (Sangher et al., 2023) illustrate and demonstrate their capability to apply sophisticated algorithms to augment cyber threat intelligence, providing a direction to incorporate new technologies into law enforcement tactics (Sangher et al., 2023). Additionally, according to (Saleem et al., 2022) knowledge on the behaviour of Darknet users would enable the design of interventions (Saleem et al., 2022 & (Abdelaziz et al., 2026)

4.7. Testing of technical and legal solutions

Continuous validation of emerging technologies (e.g., AI and ML) is likely a pivotal focus for future work. These technologies are capable of greatly improving law enforcement's ability to detect and mitigate any type of illicit activity happening on the Darknet (Soliman, 2023). Legal implications of use of these technologies are also very important which has arisen from a balancing act between monitoring and privacy rights which remains multifaceted and must be explored (Gomathy et al., 2024).

4.7. Public Health and Safety Issues

Not only does the Darknet facilitate the operation of organized crime but it has real implications for public health and safety. Study of the influence of such underground networks and the illegal activities in these underground networks on the society and individual health is needed, with drugs, trafficking and exploitation as the possible sources (Kubů, 2025) (Kubů, 2025). An understanding of how public health, crime, and the Darknet intersect could inform policy responses that are more effective.

4.8. Development Of International Legal Frameworks

Okyere-Agyei (2022) insists that the international legal systems should focus on harmonizing the legal frameworks that address the cross-border crimes

brought about by the Darknet, with a focus on linking these crimes through transnational and cross-border law that can be called upon to combat the transnational nature of crimes enabled by the Darknet (Okyere-Agyei, 2022). Focusing on developing complete legal standards and protocols is one of the most vital research areas, and international law will address the lack of consistent legal frameworks and measures, filling the enforcement and jurisdictional gaps that could also be employed to narrow the loopholes for how effective international law is against organized criminal activities.

4.9. Public Awareness and Educational Initiatives

Finally, the combination of education frameworks to educate society on the Darknet's vulnerabilities and the threat of digital anonymity can empower communities to discover and combat organized crime more effectively. As evidenced by (Kaur et al., 2024), public awareness campaigns can counteract the attractions of the dark web while also raising awareness among people about possible risks to their digital safety (Kaur et al., 2024). Based on these considerations, research must investigate the optimal protocols for implementing such integrated intervention educational methods (Brinck, 2023).

4.10. Decision Makers On Fighting Organized Crime Across Darknets.

As efforts to combat organised crime on the Darknet are on the rise, the ethics of these efforts are increasingly vital to understanding. Only an ethical, legal, and moral framework of a state's social and moral considerations is necessary to support law enforcement and state-wide-policy responses aimed at building a responsible public trust and ensuring individuals' constitutional rights and justice.

4.11. Balancing Privacy and Surveillance

One of the principal ethical questions is, does data collection comply or not with the rights of individuals? The Darknet serves as a milieu for law enforcement to participate but not only to commit malfeasance, and for them to impose or limit their personal privacy; Maheswari points out that AI in criminal investigation also needs to become transparent and respect individual rights. In the case of the data breach by policing, it may present their challenge to balance surveillance requirements with potential breaches of civil liberties within the system (Germani et al., 2024). Law enforcement is forced to create a set of guidelines that take into account the human rights principles. The technology is therefore put to good use and put into practice.

What makes more advanced technologies, such as AI in policing, both advantageous and challenging. While AI-based tools streamline investigative procedures, they must be implemented under appropriate moral standards for all these technologies to ensure that their applications are as objective and comprehensive as possible. Use of technology ethically is also necessary lest disparities remain entrenched by social justice reform and the implementation of new policies; people who are at greatest risk of suffering from policing techniques. Future studies should focus on investigating the influence of a range of these technologies in influencing moral and social values in terms of crime control and identification.

Transparency and accountability. Transparency in the targeting of the Darknet policing is essential if accountability based on perceived threats and not just on the law enforcement actions is to be established. Developing guidelines on the handling and sharing of any data obtained from Darknet investigations can play an important role in building trust. As for other types of data collection, there are problems with the use and exfiltration (Belotserkovsky, 2016) of acquired data (there is a concern that it may stigmatize and discriminate against certain groups). Constructing monitoring schemes encourages citizens to participate openly and to mitigate civil power abuse issues due to a more cooperative environment among law enforcement and communities (Germani et al., 2024).

4.12. Education and Community Engagement

Awareness programs are a major investment in the economy and in society that create and educate people about the negative consequences of organized crime in the Darknet. Educational initiatives can similarly get communities to discover threats and support constructing an intelligent perception of threats in an era of digital anonymity. This would facilitate shared accountability and involvement by communities in addressing the effects on security leading to collaborative approaches to policing—an approach based on ethical policing (not just enforcing laws, but also community security and being resilient to the organized crime) (Almahasneh, 2024).

4.13. Future Ethical Frameworks

Now we must develop a consistent moral code that is sensitive and responsive to the particular and unique issues of organized crime on the Darknet. These frameworks will promote collaborative

governance, stakeholders; engagement of tech actors; and a focus on continuous and integrated cooperation: from law enforcement, to technology actors and civil society. In this endeavour, it is crucial moral questions, must adapt along with progress of technology, would also aid formulating responses to organized crime more equitable and serving the society's need (Umakhanov & Dieva, 2023). This indicates that studies on ethical issues in public health data management could be of relevance for the establishment of robust legal practices (Ni & Korfmacher, 2025).

4.14. Recommendations for Future Ethical Policies and Research Directions

The growing moral and procedural challenges faced by organized crime on the Darknet also exacerbate the need for ethical policies, principles and models that promote addressing criminal activity along with protecting individual rights simultaneously, which corresponds with the growth of digital crime. The recommendations below will aid in guiding policymakers, law enforcement, and researchers to promote measures that are effective and ethical.

For policing, the definition of ethical guidelines is about the development of standards which serve to expand ethical guidelines for conduct of law enforcement.

Laws must be good ethical principles to manage law enforcement in relation to Darknet crimes. These ideals need to properly protect your civil liberties and also work to permit investigation and surveillance. Transparency, accountability and privacy are fundamental principles that should become institutionalized in such regimes (Raymen, 2015). Another part should be to establish specialized training programs to ensure that the department members possess the training needed to make ethical decisions with public confidence, in harmony with the models of ethical decision-making specified in Dempsey et al.

Awareness and general education campaigns to promote community learning and growth. Public dialogue regarding dangers of digital behaviour and its effects would help community members learn better online behaviours. Education from the public should be addressed through public education about dangers of the Darknet. Moreover, inclusive public dialogue would promote the community's feedback regarding the ethical dimensions of policing leading to a community-based crime prevention and response process (Bunei, 2017).

Stakeholder Partnership and Collaboration

In order to address the multidimensional nature of darknet organized crime it is necessary for different sectors, the academia and the private sector, CSE and law enforcement to come together. These partnerships are essential if we are to deliver holistic solutions that combine innovation with law and ethics. This in turn enables responses that adhere to human rights at every aspect of policy formulation/reform and policing (Denno, 1987). Combining different knowledge across a number of domains gives us better solutions that can respond to diverse stakeholder needs. Continuing Ethical Research and Policy Adaptive Strategies

It is essential to ensure that ongoing ethical research into the ethics of addressing cyber-criminal organizations and the need to develop policy interventions focused on ethical guidelines should be kept going. It will be helpful for continued monitoring and evaluation of current policies and interventions to adapt to constantly changing technological environments with those necessary alterations. Subsequent research should evaluate the efficacy of interventions and their socio-ethical implications, so as not to criminalize personal liberty and contribute to public order that would not be violated by deviance reduction—thus avoiding its occurrence (Us et al., 2024).

4.15. Technology in the Right Manner

New technologies, including artificial intelligence and data analytics, for crime prevention must also be implemented with extreme ethical sensitivity with fairness and bias paramount. Policymakers need to collaborate with technology companies to guarantee that this innovative technology does the justice while preventing invasive monitoring practices that adversely affect the underprivileged (Luong, 2024). Clearly establishing guidelines for ethical practices when employing these technologies is the first essential step towards avoiding erosion of public trust and incompliance with human rights-oriented strategies. Closing: Key Takeaways and Recommendations

5. CONCLUSION: KEY FINDINGS AND RECOMMENDATIONS

Last, the current study delineates the multi-layered role of the Darknet in facilitating organized crime, identifying the many-pronged challenges that the law enforcement and the legal system organisations encounter outside their jurisdictions. Based on this data, the underlying characteristics of anonymity and decentralization of Darknet, especially individuals on Tor, produce a platform

designed for criminal activity to take place without much surveillance (Luong, 2024; Bertola, 2020). These features can make it impossible to catch and prosecute criminals as well. In addition, the Darknet associated with organized crime is characterized by a dense web comprising multiple networks and a digital networked infrastructure less dependent on hierarchical or geographic structures (Bancroft, 2020; Hartmann, 2025). Add to these issues the disparities of jurisdiction and the fragmentation of the legal structures among the countries, which hinders coordinated responses and creates loopholes to the criminal (European Union, 2008; Khobbi et al., 2022). This ethical issue does not obviate law enforcement from having an ethical problem; law enforcement surveillance along with the privacy and technology ethics should also not be considered to have insufficient control, on the contrary public trust in and a right to basic human rights is threatened (Soliman, 2023; Lyngstad & Skarðhamar, 2010). In order to meet the challenges, governments must develop adaptable and mature regulatory frameworks in line with the explosive growth of cybercrime and harmonize global norms to enable collective enforcement (Kougiannou & Ridgway, 2021). High-grade surveillance processes such as AI, big data analysis, blockchain forensics and specialized professional training in these methods should be built of and developed and maintained in order to increase police capacity and efficiency in an ever-evolving environment (Luong, 2024). Knowledge of Darknet and digital literacy, including general school courses, education programs designed to sensitize the public to the dangers of the Darknet, must be available to allow them to report suspicious behavior and to use them without delay (Pocock & Phua, 2011). Furthermore, it is important to encourage collaboration among universities, tech organizations, civil society and police departments, to provide the type of sharing of knowledge, innovation and best practices necessary to share and utilise their collective responses to Darknet enabled crime (Kougiannou & Ridgway, 2021). Establishment of and enforcing transparent, ethical parameters that guide law enforcement operations should promote a transparent and accountable form of law enforcement. As civil liberties are respected under this approach, its impact will be greater too (Lyngstad & Skarðhamar, 2010). Moreover, continued interdisciplinary research on ethical dimensions of law enforcement in today's digital age will be an essential function in guiding policy and improving practice (Lowery & Gautam, 2025). In short, dealing with the multi-dimensional complexities involved with Darknet facilitated organized crime necessitates a holistic approach. This includes taking on legal advances together with improvements in technology, ethical vigilance, and inter-related services that complement law enforcement practices. This holistic approach, by bringing all stakeholders together and allowing everyone to work towards a safer digital environment, they can work for justice and also secure those individual rights and freedoms that ensure the right to justice while still taking a respectful stance towards these individualistic human rights and freedoms that guarantee this justice.

Acknowledgements: The author would like to express sincere gratitude to Prince Sultan University, Riyadh, Saudi Arabia, for its invaluable support and resources. special thanks to the Governance and Policy Design Research Lab (GPDRL) of Prince Sultan University (PSU) for their financial and academic support to conduct this research and publish it in a reputable Journal.

Funding: This research was financially supported by the Governance and Policy Design Research Lab (GPDRL) at Prince Sultan University, Riyadh, Saudi Arabia.

Competing Interests: The author declares that there are no competing interests

REFERENCES

Abdelaziz, D. K. A., Bhouri, H., & Yaghi, R. (2026). Deepfake as an emerging crime: A victimological perspective. Scientific Culture, https://sci-cult.net/index.php/cult/article/view/1624/1111

Abdulrauf, L. (2018). The challenges for the rule of law posed by the increasing use of electronic surveillance in Sub-Saharan Africa. African Human Rights Law Journal, 18(1). https://doi.org/10.17159/1996-2096/2018/v18n1a17

Achek, I., Khelil, I., & Khlif, H. (2026). Money laundering and auditing: A survey of empirical literature. Journal of Financial Reporting and Accounting. https://doi.org/10.1108/JFRA-09-2025-0769

Adel, A., & Norouzifard, M. (2024). Weaponization of the growing cybercrimes inside the Dark Net: The question of detection and application. Big Data and Cognitive Computing, 8(8), 91. https://doi.org/10.3390/bdcc8080091

Bakken, S., Moeller, K., & Sandberg, S. (2017). Coordination problems in cryptomarkets: Changes in cooperation, competition and valuation. European Journal of Criminology, 15(4), 442–460. https://doi.org/10.1177/1477370817749177

Belotserkovsky, S. (2016). On the criminological foundations of legal regulation of combating organized crime. Russian Journal of Legal Studies (Moscow), 3(2), 187–192. https://doi.org/10.17816/rjls18169

Bertola, F. (2020). Drug trafficking on darkmarkets: How cryptomarkets are changing drug global trade and the role of organized crime. American Journal of Qualitative Research, 4(2), 27–34. https://doi.org/10.29333/ajqr/8243

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

Bunei, E. (2017). The hunt for the precious wood. Society and Business Review, 12(1), 63–76. https://doi.org/10.1108/sbr-04-2016-0025

Buszko, A. (2020). Transformation towards a market-oriented economy – An impetus or hindrance for organized crime in Poland? Olsztyn Economic Journal, 15(1), 5–22. https://doi.org/10.31648/oej.5395

Ceylan, S., & Çetinkaya, B. (2019). Attitudes towards gossip and patient privacy among paediatric nurses. Nursing Ethics, 27(1), 289–300. https://doi.org/10.1177/0969733019845124

Dempsey, R., Eskander, E., & Dubljević, V. (2023). Ethical decision-making in law enforcement: A scoping review. Psych, 5(2), 576–601. https://doi.org/10.3390/psych5020037

Décary-Hêtu, D., Faubert, C., Chopin, J., Malm, A., Ratcliffe, J., & Dupont, B. (2023). "Like aspirin for arthritis": A qualitative study of conditional cyber-deterrence associated with police crackdowns on the dark web. Criminology & Public Policy, 22(4), 639–664. https://doi.org/10.1111/1745-9133.12642

Dearden, T., & Tucker, S. (2023). Follow the money: Analyzing darknet activity using cryptocurrency and the bitcoin blockchain. Journal of Contemporary Criminal Justice, 39(2), 257–275. https://doi.org/10.1177/10439862231157521

Dhali, M., Hassan, S., Mehar, S. M., Shahzad, K., & Zaman, F. (2023). Cryptocurrency in the Darknet: Sustainability of the current national legislation. International Journal of Law and Management. https://doi.org/10.1108/IJLMA-09-2022-0206

Ditta, M. (2017). Platform criminalism: The "last-mile" geography of the darknet market supply chain. https://doi.org/10.48550/arxiv.1712.10068

Dutta, B. (2025). Insider trading and organized crime: A legal and regulatory perspective. Journal of Informatics Education and Research, 5(2). https://doi.org/10.52783/jier.v5i2.2445

El-Kady, R. (2024). Leveraging artificial intelligence to combat illicit activities on the dark web. In Advances in Digital Crime and Forensics (pp. 365–392). 10.4018/979-8-3693-9591-2.ch013

Eskens, S. (2020). The personal information sphere: An integral approach to privacy and related information and communication rights. Journal of the Association for Information Science and Technology, 71(9), 1116–1128. https://doi.org/10.1002/asi.24354

Franata, H., & Santiago, F. (2022). Authority of taping as a tool of evidence in criminal acts of corruption in Indonesia. Journal of World Science, 1(11), 1025–1030. https://doi.org/10.58344/jws.v1i11.135

Gannon, C., Blokland, A., Huikuri, S., Babchishin, K. M., & Lehmann, R. (2023). Child sexual abuse material on the darknet. Forensische Psychiatrie, Psychologie, Kriminologie, 17(4), 353–365. https://doi.org/10.1007/s11757-023-00790-8

Germani, F., Spitale, G., Machiri, S., Ho, C., Ballalai, I., Biller-Andorno, N., … & Reis, A. (2024). Ethical considerations in infodemic management: Systematic scoping review. JMIR Infodemiology, 4, e56307. https://doi.org/10.2196/56307

Gomathy, C., Geetha, D., Chakravarthi, M., & Kumar, M. (2024). Navigating the shadows: Unraveling the legal and ethical challenges of the dark web and cryptocurrency. International Journal of Scientific Research in Engineering and Management, 08(09), 1–6. https://doi.org/10.55041/ijsrem37511

Goonetilleke, P., Knorre, A., & Kuriksha, A. (2023). Hydra: Lessons from the world's largest darknet market. Criminology & Public Policy, 22(4), 735–777. https://doi.org/10.1111/1745-9133.12647

Gundur, R., Berry, M., & Taodang, D. (2021). Using digital open source and crowdsourced data in studies of deviance and crime. In Advances in Criminology (pp. 145–167). https://doi.org/10.1007/978-3-030-74837-1_8

Harrison, J., Roberts, D., & Hernández-Castro, J. (2016). Assessing the extent and nature of wildlife trade on the

dark web. Conservation Biology, 30(4), 900–904. https://doi.org/10.1111/cobi.12707
Hartmann, A. (2025). From syndicates to protocols: Rethinking organized crime in the age of cybercrime. International Journal of Criminology and Sociology, 14, 116–128. https://doi.org/10.6000/1929-4409.2025.14.11
Hiramoto, N., & Tsuchiya, Y. (2022). Are illicit drugs a driving force for cryptomarket leadership? Journal of Drug Issues, 53(3), 451–474. https://doi.org/10.1177/00220426221133030
Jardine, E. (2021). Policing the cybercrime script of darknet drug markets: Methods of effective law enforcement intervention. American Journal of Criminal Justice, 46(6), 980–1005. https://doi.org/10.1007/s12103-021-09656-3
Jardine, E., Lindner, A., & Owenson, G. (2020). The potential harms of the Tor anonymity network cluster disproportionately in free countries. Proceedings of the National Academy of Sciences, 117(50), 31716–31721. https://doi.org/10.1073/pnas.2011893117
Javed, M., Hussain, N., & Maitla, M. (2021). CCTV cameras surveillance, data protection & privacy under international human rights laws. Journal of Law & Social Studies, 3(2), 174–186. https://doi.org/10.52279/jlss.03.02.174186
Kaushik, K. (2022). Dark web: A playground for cyber criminals. CJACSIT, 2(1), 44–52. https://doi.org/10.17492/computology.v2i1.2206
Kaur, G., Mukherjee, D., Moza, B., Pahwa, V., Kaur, K., & Kaur, K. (2024). The dark web: A hidden menace or a tool for privacy protection. IP International Journal of Forensic Medicine and Toxicological Sciences, 8(4), 160–167. https://doi.org/10.18231/j.ijfmts.2023.034
Kethineni, S., & Cao, Y. (2019). The rise in popularity of cryptocurrency and associated criminal activity. International Criminal Justice Review, 30(3), 325–344.https://doi.org/10.1177/1057567719827051
Khan, S., Zakir, M., Tayyab, A., & Ibrahim, S. (2024). The role of international law in addressing transnational organized crime. J. Asian Dev. Studies, 13(1), 283–294. https://doi.org/10.62345/jads.2024.13.1.24
Khobbi, Y., Сторожук, I., Svoboda, I., Kuzmenko, S., & Tymchyshyn, A. (2022). Reforming techniques to combat organized crime in the context in view of securing human rights and freedoms. Cuestiones Políticas, 40(73), 192–214. https://doi.org/10.46398/cuestpol.4073.09
Kougiannou, N., & Ridgway, M. (2021). How is human resource management research (not) helping practice? In defence of practical implications. Human Resource Management Journal, 32(2), 470–484. https://doi.org/10.1111/1748-8583.12414
Kubů, P. (2025). Aktuální rizika a možné přínosy darknetu pro individuální i veřejné zdraví. Medsoft. 10.35191/medsoft_2025_1_37_kubu
Lowery, C., & Gautam, C. (2025). K12 superintendent awareness of critical race theory: Perspectives, perceptions, and presumptions. Educational Administration Quarterly, 61(3), 400–433. https://doi.org/10.1177/0013161x241308525
Leukfeldt, R., & Holt, T. (2019). Examining the social organization practices of cybercriminals in the Netherlands online and offline. International Journal of Offender Therapy and Comparative Criminology, 64(5),522–538. https://doi.org/10.1177/0306624x19895886
Luong, H. T. (2024). Foundations and trends in the darknet-related criminals in the last 10 years: A systematic literature review and bibliometric analysis. Security Journal. https://doi.org/10.1057/s41284-023-00383-4
Maheswari, A. U. (2025). Artificial intelligence and its ethical implications in global society: A conceptual exploration. Artificial Intelligence, https://doi.org/10.51584/IJRIAS.2025.10060092
NordPass. (2025). Insights from the 2025 EU SOCTA. Retrieved from https://nordpass.com/blog/the-changing-dna-of-organized-crime-in-europe/
Oosthoek, K., Staalduinen, M., & Smaragdakis, G. (2023). Quantifying dark web shops' illicit revenue. IEEE Access, 11, 4794–4808. https://doi.org/10.1109/access.2023.3235409
Pocock, N., & Phua, K. (2011). Medical tourism and policy implications for health systems: A conceptual framework from a comparative study of Thailand, Singapore and Malaysia. Globalization and Health, 7(1), 12. https://doi.org/10.1186/1744-8603-7-12
Raymen, T. (2015). Designing-in crime by designing-out the social? Situational crime prevention and the intensification of harmful subjectivities. The British Journal of Criminology, 56(3), 497–514. https://doi.org/10.1093/bjc/azv069
Saleem, J., Islam, R., & Kabir, M. (2022). The anonymity of the dark web: A survey. IEEE Access, 10, 33628–

33660. https://doi.org/10.1109/access.2022.3161547

Sangher, K., Singh, A., Pandey, H., & Kumar, V. (2023). Towards safe cyber practices: Developing a proactive cyber-threat intelligence system for dark web forum content by identifying cybercrimes. Information, 14(6), 349. https://doi.org/10.3390/info14060349

Shevchuk, H., & Voluiko, O. (2025). Administrative approach to preventing organized crime: European experience and prospects for Ukraine. Analytical and Comparative Jurisprudence, 2(3), 314–320. https://doi.org/10.24144/2788-6018.2025.03.2.50

Soliman, M. (2023). Layers of the internet: The challenge of the dark web and the need for an international legal framework. International Journal of Cryptocurrency Research, 3(1), 74–77. https://doi.org/10.51483/ijccr.3.1.2023.74-77

Tennant, I. (2021). Fulfilling the promise of Palermo? A political history of the UN convention against transnational organized crime. Journal of Illicit Economies and Development, 2(1), 53–71. https://doi.org/10.31389/jied.90

Tovino, S. (2020). Privacy and security issues with mobile health research applications. The Journal of Law Medicine & Ethics, 48(S1), 154–158. https://doi.org/10.1177/1073110520917041

Tzanetakis, M., & Marx, S. (2023). The dark side of cryptomarkets: Towards a new dialectic of self-exploitation within platform capitalism. https://doi.org/10.1108/978-1-80043-866-820231010

Umakhanov, J., & Dieva, M. (2023). Criminological features organized counterfeiting in the digital age. Russian Studies in Law and Politics, 7(3), 18–33. https://doi.org/10.12731/2576-9634-2023-3-18-33

Wang, Y., Arief, B., & Hernandez-Castro, J. (2021). Toad in the hole or Mapo tofu? Comparative analysis of English and Chinese darknet markets. https://doi.org/10.1109/ecrime54498.2021.9738745

Weitz, J., Hammerl, L., Halms, T., Rabenstein, A., Rüther, T., Hasan, A., … & Gertzen, M. (2025). Procurement pathways of illegal substances in Germany: A systematic review with implications for prevention, harm reduction, and drug policy. Current Addiction Reports, 12(1). https://doi.org/10.1007/s40429-025-00671-6