Journal of Communication and Management

ISSN: 2583-617X (Online)

Journal home page: https://jcoma.com

Research Article **DOI: 10.58966/JCM2025436**

Hidden Side of the Internet: Between Crime and Freedom on the Dark-Web

Arun Kumar Gond*

Department of Sociology, University of Allahabad, Prayagraj, Uttar Pradesh, India

ARTICLE INFO

Article history:

Received: 26 July, 2025

Revised: 18 July, 2025

Accepted: 25 August, 2025

Published: 22 September, 2025

Keywords:

Dark-web, Tor Browser, Cybercrime, Digital Criminology, Web Scraping, Digital Literacy, Online Anonymity, Hidden Internet.

ABSTRACT

The dark-web is a hidden subset of the deep-web, inaccessible through conventional search engines and reachable only via anonymizing browsers like Tor (The Onion Router). While originally developed to protect user privacy, the dark-web has become notorious for hosting illegal activities such as drug trafficking, child exploitation, arms trade, and extremist recruitment. At the same time; it also serves as a space for whistleblowers, journalists, and those seeking digital anonymity in repressive regimes. Studying this concealed domain is vital for understanding the broader landscape of cybercrime and digital risk. This paper presents a theoretical and methodological exploration of the dark and deep web, focusing on access barriers, ethical concerns; and the role of technology in uncovering hidden data. It emphasizes the importance of advanced tools such as web scraping, and specialized search engines in responsibly navigating these complex spaces. Furthermore; the study highlights the significance of digital literacy and ethical awareness in ensuring that research in such environments does not replicate harm or violate user rights. Through a combination of surveillance studies, digital criminology, and information science, the research advocates for interdisciplinary collaboration to better interpret and engage with the dark-web.

Introduction

The internet has changed the way people talk, buy things, and find information. Most people use the surface websites like Google, Facebook, and Amazon. But there is another hidden part of the internet that many people do not know much about. This is called the Dark-web. It is often shown in movies and news as a scary and dangerous place; but it is more complex than that. The Dark-web is a secret area of the internet where people can stay anonymous. It cannot be found using regular web browsers or search engines (Ngo et al., 2023). The Dark-web works through special software like TOR (The Onion Router). This software hides a user's identity by passing their information through many different computers around the world. This makes it hard to trace where the user is or what they are doing. Because of this, the Dark-web can protect people's privacy. It is often used by journalists, whistleblowers, and activists who live in countries where free speech is not allowed. These people use the Dark-web to share information without getting caught. However, the same tools that protect good people can also be used for bad purposes[1]. Some criminals use the Dark-web to sell drugs, weapons, or stolen data. There are also secret websites where illegal activities happen, like identity theft, scams, and even hiring criminals. Because it is so hard to trace people on the Dark-web; law enforcement finds it difficult to catch them (Curtis & Oxburgh, 2022). But it is important to understand that the Dark-web itself is not illegal. It is just a tool, and like any tool, it can be used in both good and bad ways. The Dark-web raises big questions about privacy, freedom, and safety on the internet. In today's world, where governments and companies can watch what we do online, the Dark-web shows us why many people still care about being anonymous. In short, the Dark-web is a secret part of the internet. It can help

***Corresponding Author:** Arun Kumar Gond

Address: Department of Sociology, University of Allahabad, Prayagraj, Uttar Pradesh, India

Email ✉**:** arungond413@gmail.com

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

protect freedom and privacy; but it can also hide criminal acts (Gehl, 2014). To understand the future of the internet, we must learn more about what the Dark-web really is and how it is used.

Defining the Dark-web

The Dark-web is commonly defined as the portion of the Deep-Web that is deliberately hidden and inaccessible through standard browsers and search engines. While the Deep-Web encompasses any content not indexed by traditional search engines (such as academic databases, subscription services, or private intranets); the Dark-web is a subset of this unindexed space that requires specific software, configurations, or authorization to access (Gadek et al., 2018). The most well-known entry point is through The Onion Router (TOR), a software that anonymizes users by routing their internet traffic through multiple encrypted layers of servers, thereby masking their IP addresses. The term "Darknet", often used interchangeably with Dark-web, originally emerged in the 1970s to refer to isolated computer networks that were not connected to ARPANET (the precursor of the modern internet)[2]. Over time, this term evolved to refer to peer-to-peer encrypted networks that allow users to exchange information privately, with little risk of detection[3]. The Dark-web, then, is not a single unified space but a collection of hidden websites and services that rely on such anonymizing technologies for their operation and protection (Davies, 2020).

The history of the Dark-web is intricately linked to the development of the modern internet. Its origins can be traced back to the 1960s and 70s, when the Advanced Research Projects Agency Network (ARPANET) was established by the U.S. Department of Défense as a military-grade academic research network (Warf, 2018). In the early stages, privacy was not a primary concern; but by the 1980s and 90s; as the internet became more commercialized- the need for private, secure, and decentralized communication began to rise, particularly among activists, researchers, and those seeking protection from state surveillance (Merrill, 2024). The 1990s saw rapid developments in encryption, storage, and file-sharing technologies, leading to the rise of underground forums, bulletin boards, and private sharing networks. The concept of data havens; locations or servers operating beyond legal jurisdictions- also emerged, facilitating the hosting of content otherwise illegal in certain countries, including pornography, gambling, and politically sensitive materials[4]. A significant turning point came in 2002, when the TOR project was officially released, sponsored initially by the U.S. Naval Research Laboratory. Designed to protect online communications and promote free expression, TOR allowed users to access the internet without revealing their identity (Collier, & Stewart, 2021). Ironically, while TOR was developed to support democratic movements and journalistic freedom, it also inadvertently created an infrastructure ripe for misuse by criminal elements, enabling marketplaces for illicit goods, stolen data, and cybercrime. Today, alongside TOR, other anonymizing networks such as the Invisible Internet Project (I2P) and Freenet have further diversified the ways in which users can access the Dark-web (Dencik et al., 2016). These technologies are unified by a commitment to decentralization, anonymity, and encryption, making them both powerful tools for civil liberties and potential threats to law enforcement and national security. The Dark-web presents a unique moral and legal conundrum. On one hand, it is heralded as a liberating space for journalists, political dissidents, and whistleblowers operating under repressive regimes. For example, platforms like Secure Drop- hosted on TOR- allow individuals to leak information safely to media outlets. Similarly, marginalized communities often turn to these platforms to seek help, community, or organize resistance (Madouh & Kwon, 2023). On the other hand, the anonymity afforded by the Dark-web has made it a fertile ground for illicit trade and harmful activity. Dark-web markets like Silk Road, Alpha Bay; and Hansa have been notorious for facilitating the sale of illegal drugs, firearms, counterfeit goods, stolen data, and even contract killing services. While many of these marketplaces have been shut down by international law enforcement, others continue to emerge in their place, increasingly using cryptocurrencies such as Bitcoin and Monero to facilitate untraceable transactions. Moreover, the Dark-web is a site of digital extremism, hosting forums and communities that promote radical ideologies, terrorism, and hate speech (Howell et al., 2023). Its inaccessibility to regular users; and its resistance to surveillance pose serious challenges to cybersecurity, digital governance, and law enforcement efforts worldwide.

Scope of the Dark-web

The dark-web is a hidden part of the internet that most people don't see or use in their daily lives. You can't find it through normal search engines like Google. To enter it, you need special tools like the Tor browser, which helps people stay anonymous online. The dark-web is not always bad. Some people use it for good reasons. For example; journalists and whistleblowers use it to share information safely, especially in countries were speaking out can be dangerous. It helps protect their identity and keeps them safe from harm. But the dark-web is also known for illegal things. Many people use it to buy or sell drugs, weapons, fake documents, or stolen data. Hackers offer their services here; and there are forums that promote dangerous or harmful content (Koenraadt & van de Ven, 2017). Because users are anonymous and payments are made through cryptocurrency like Bitcoin, it's hard for police and investigators to track them down. So, the dark-web has two sides. On one hand, it can protect freedom of speech and privacy. On the other hand; it can hide dangerous crimes.

That's why it's important to understand both the legal and illegal uses of the dark-web. When we study the dark-web, we need to look at the full picture; not just the scary parts. This helps us find better ways to protect people and stop online crime without taking away the right to privacy.

Relevance in Contemporary Society

In today's digitized world, where surveillance capitalism and algorithmic control dominate online spaces, the Dark-web also symbolizes a form of resistance to mainstream internet norms. The monopolization of data by corporations; and state actors has raised urgent questions about digital rights, privacy, and freedom of expression (Kwon et al., 2021). Within this context, the Dark-web represents both a solution and a problem- a site of potential emancipation as well as peril. Academically, the Dark-web has become an increasingly important subject of interdisciplinary study, drawing interest from criminologists, sociologists, cybersecurity experts, legal scholars, and media theorists. As the boundaries between legality and illegality, visibility and invisibility, public and private blur online, understanding the Dark-web becomes essential not just for policing crime but for rethinking the future of digital citizenship (Bradshaw & Howard, 2019). It is crucial, however, not to view the Dark-web merely as a "criminal underworld." Such reductionist interpretations overlook the structural and systemic factors- such as censorship, lack of digital freedom, geopolitical oppression, and economic inequality- that drive individuals and communities toward these hidden spaces. The Dark-web is not a monolith. It is a dynamic, contested, and complex digital terrain- one that reflects the best; and worst of human impulses in the information age. As this paper explores in the following sections, the Dark-web must be understood not only through the lens of crime and deviance, but also through the sociotechnical frameworks of resistance, surveillance, encryption, and digital justice (Frischlich et al, 2019). The central objective is to unpack the technological infrastructures (like TOR, I2P, and Freenet) that sustain the Dark-web, analyse the role of cryptocurrencies in facilitating its underground economy; and critically reflect on the dual-use nature of anonymized digital spaces in an increasingly polarized world.

Literature Review

Nearchos's book *Combating Crime on the Dark-web* (2023) presents a structured and comprehensive investigation into the multifaceted world of cybercrime, emphasizing the sociotechnical dynamics of the Dark-web. The work is divided into three parts, each exploring a distinct aspect of the Dark-web ecosystem, its criminal potential, and global countermeasures. Author traces the evolution of cybercriminal methods in tandem with digital infrastructure, identifying three layers of the internet: Surface Web, Deep Web, and Dark-web (p. 8). A strength of this section lies in its clear explanation of anonymizing technologies like the TOR browser (pp. 15–20), I2P, and Freenet (pp. 20–21), showing how these tools simultaneously protect privacy and facilitate illegal operations (Nearchou, 2023). Notably, Author proposes a centralized intelligence system (IDH) for monitoring and mitigating Dark-web threats (pp. 98–104), raising important questions about surveillance ethics, digital governance, and privacy. Overall, the book serves as a valuable resource for scholars and policymakers alike. For Indian researchers; particularly those studying cybercrime in rural or semi-urban contexts, the book's emphasis on encryption, decentralized platforms, and jurisdictional challenges offers a compelling lens through which to analyse emerging digital risks and regulatory gaps.

Ben Collier's *TOR: From the Dark-web to the Future of Privacy* (2022) is an important sociotechnical study that explores how the Tor network has shaped global ideas about privacy, surveillance, and internet freedom. Rather than viewing Tor only as a tool to access the Dark-web, Author presents it as a complex system where politics, ethics, and technology meet. He shows how Tor has grown from a U.S. (Collier, 2022). One of Author's key arguments is that privacy is not just a personal right, but a space of struggle between different actors—such as governments, corporations, and civil society. He introduces the idea of 'privacy worlds,' where each group builds its own vision of what privacy should look like. He also explains that technologies like Tor are never neutral; they carry values, assumptions, and political choices. Author mixes technical explanations with social theory. He explains Tor's onion routing system clearly while also analysing how communities maintain and shape the network. He critiques the media for often presenting Tor and the Dark-web in a sensationalist way, especially in discussions around crime and extremism. Instead, he emphasizes that problems on the Dark-web reflect wider social issues. Overall, this book is a strong contribution to digital sociology and privacy studies. It helps readers understand how digital infrastructures are created, maintained, and contested, and why tools like Tor will remain central to future debates on online freedom.

Gaps in Literature

Although there is growing research on cybercrime and the Dark-web, many gaps remain. Most existing studies focus heavily on technical or legal aspects, like hacking methods or law enforcement strategies. What's often missing is a deeper understanding of the social and cultural side; how ordinary people interact with hidden digital spaces; and how factors like class, education, or digital literacy shape their online behaviour. Very few studies explore the real-life experiences of users who may unknowingly

fall into dangerous spaces on the Dark-web. Also, there is limited research on how the Dark-web effects developing countries, where awareness and access to digital security tools are often low. This paper aims to fill these gaps by connecting theories from sociology, surveillance studies, and digital criminology, offering a more complete picture of how hidden internet spaces impact daily life and public safety.

Methodology: Theoretical Framework Approach

This study uses a theoretical approach instead of fieldwork or data collection. Rather than doing surveys or interviews; it focuses on thinking deeply about ideas and concepts to understand how people use hidden parts of the internet especially the Dark-web; and how that affects everyday life (Papacharissi, 2015; Gehl, 2018). The research is based on three main frameworks; *Surveillance*: helps us understand how people use tools like Tor, VPNs, and encrypted apps to stay hidden online. Many users don't fully know how digital surveillance works. This theory shows how people feel about their privacy, how they try to avoid being watched, and how data tracking often happens without their awareness (Rainie & Wellman, 2019). It also questions the belief that privacy online is ever fully secure. *Digital Criminology*: This framework looks at the kinds of crimes happening on the Dark-web; like identity theft, drug sales, child exploitation, or online fraud. It also helps us understand how ordinary people may unknowingly become victims or part of these systems. It draws attention to low digital awareness, lack of legal knowledge, and gaps in protection, especially for vulnerable users (Swart et al., 2018). *Sociology:* gives a bigger picture. It helps us see how class, gender, education, and access to technology affect how people understand and use the internet. Not everyone experiences the digital world equally. Some people are more at risk because of social or economic barriers (Castells, 2010). By using these three perspectives together, the study explores how culture and technology are shaping our digital lives; and why we need stronger digital education, public awareness, and smart policies to face the risks that come with the hidden web.

Core Sections

History and Evolution of the Dark-web

The Dark-web's origins trace back to the 1960s with the development of ARPANET (Advanced Research Projects Agency Network), an early packet-switching network and a precursor to the modern internet. Initially designed for secure communication among U.S. military and research institutions; ARPANET laid the groundwork for future anonymous networks. In the 1990s, the concept of anonymous communication gained traction, leading to the development of technologies that would eventually support the Dark-web[5]. The term "Darknet" emerged to describe networks not indexed by standard search engines and accessible only through specific configurations or software. A significant milestone was the release of The Onion Router (TOR) in the early 2000s. TOR was developed to provide users with anonymity online by routing their communications through a network of volunteer-operated servers; masking their identities and locations (Chen et al., 2022). This technology became the backbone of the Dark-web, enabling users to access hidden services and websites with. Onion domains.

Technologies Enabling Anonymity

TOR operates on the principle of "onion routing," where data is encrypted in multiple layers and transmitted through a series of nodes or relays. Each node peels away a layer of encryption; revealing the next destination, until the data reaches its final endpoint. This process ensures that no single node knows both the origin and destination of the data, preserving user anonymity. While TOR provides robust privacy features, it has some drawbacks: Speed Limitations: Routing through multiple nodes can slow down internet speeds. Potential for Misuse: While TOR is a tool for privacy; it's also used for illicit activities (Eklund et al., 2021). Vulnerabilities at Exit Nodes: Data exiting the TOR network can be intercepted if not encrypted, posing security risks.

I2P and Freenet

Comparison and Functionality

I2P (Invisible Internet Project) is designed for secure internal communications within its network. Unlike TOR, which allows access to the regular internet; I2P focuses on anonymous peer-to-peer connections, making it suitable for activities like blogging, file sharing, and messaging within its ecosystem. Freenet emphasizes decentralized data storage. Users contribute storage space, creating a distributed network where content is stored and retrieved anonymously (Schriner, 2019). Freenet is particularly resilient against censorship, as data is spread across numerous nodes. Accessibility: TOR allows access to both the Dark-web and the regular internet; I2P and Freenet are more insular. Use Cases: TOR is versatile; I2P is ideal for internal services; Freenet excels in anonymous data storage. Performance: TOR and I2P offer better speeds; Freenet may experience latency due to its storage mechanism. The balance between maintaining user anonymity and enabling surveillance for security purposes is delicate. While technologies like TOR, I2P, and Freenet empower users to protect their privacy; they also pose challenges for law enforcement agencies attempting to monitor criminal activities (Hegarty, 2025). This ongoing tension underscores the complexities of digital privacy in the modern age.

Cryptocurrencies and the Economy of the Dark-web

Cryptocurrencies have become integral to the Dark-web's

economy due to their pseudonymous nature. Bitcoin was the first cryptocurrency widely adopted for transactions on the Dark-web, offering users a way to exchange value without traditional banking systems. However, Bitcoin's transparency on the blockchain has led to the adoption of more privacy-focused cryptocurrencies like Monero and Zachs. These coins offer enhanced anonymity features; making it more challenging to trace transactions. The anonymous nature of cryptocurrency transactions complicates efforts to combat illegal activities on the Dark-web (Dearden & Tucker, 2023). Law enforcement agencies face difficulties in tracking and prosecuting crimes due to; *Obscured Transaction Trails:* Privacy coins conceal sender and receiver information. Decentralization: The lack of a central authority makes regulation and oversight challenging. Global Reach: Transactions can occur across borders; complicating jurisdictional enforcement. Efforts are ongoing to develop tools and frameworks to monitor and regulate cryptocurrency use without infringing on legitimate privacy rights (Androulaki et al., 2013).

Legal, Ethical, and Social Implications

The Dark-web exemplifies the broader debate between individual privacy rights and the need for surveillance to ensure security. Advocates argue that tools like TOR protect freedom of expression and privacy, especially in oppressive regimes. Critics highlight the Dark-web's role in facilitating illegal activities; emphasizing the need for oversight (Badhwar, 2021). Government Policies and Technological Challenges; Governments worldwide grapple with regulating the Dark-web; Legislation: Laws targeting cybercrime and digital anonymity vary by country, leading to inconsistent enforcement. *Technological Hurdles*: The evolving nature of encryption and anonymity tools outpaces regulatory measures. *Ethical Considerations*: Balancing civil liberties with security measures remains a contentious issue (Chen et al., 2019). Collaborative international efforts and adaptive policies are essential to address the multifaceted challenges posed by the Dark-web.

Dark-web and Criminal Activities

The Dark-web hosts a range of illegal activities, including: Drug Trafficking: Online marketplaces facilitate the sale of narcotics. *Weapons Trade*: Firearms and explosives are traded anonymously. *Human Trafficking*: Platforms enable the exploitation of individuals. Cybercrime Services: Hacking tools, malware, and stolen data are available for purchase (Hiramoto & Tsuchiya, 2020). *Illegal Pornography*: The distribution of explicit and often illegal content occurs in hidden forums. Law Enforcement and Prosecution Challenges Combating crime on the Dark-web presents unique obstacles; *Anonymity:* Users' identities are concealed, hindering investigations. *Jurisdictional Issues*: Crimes often span multiple countries, complicating legal proceedings. *Resource Limitations*: Specialized skills and tools are required to infiltrate and monitor Dark-web activities (Sayyed & Paul, 2025). Despite these challenges, law enforcement agencies have achieved notable successes, such as dismantling major marketplaces like Silk Road and Alpha Bay; demonstrating the potential for effective intervention.

Discussion

The Dark-web is a hidden part of the internet that cannot be accessed through regular browsers like Google Chrome or Firefox. To visit it, people use tools such as the Tor browser, which helps keep their identity private. Websites on the Dark-web are not listed on search engines and are often encrypted for anonymity. Many people associate the Dark-web with illegal activities; and for good reason. It has been used for selling drugs, weapons, fake documents, and stolen data. There are also serious crimes like child exploitation and financial fraud that take place in these hidden spaces (Chaves & Gerosa, 2020). High-profile cases like the Silk Road; a major illegal marketplace shut down in 2013; have reinforced the belief that the Dark-web is a dangerous and criminal zone. But this is only part of the story. The Dark-web also has positive uses; especially for people living under strict or oppressive governments. In such countries, where speaking freely can lead to arrest or violence, the Dark-web becomes a tool for survival. It allows journalists, whistleblowers, and human rights activists to share information without fear (Jørgensen & Desai, 2017). Platforms like Secure Drop give whistleblowers a safe space to expose corruption while protecting their identity. Privacy is another important reason why some people choose the Dark-web. On the regular internet, our activities are tracked by tech companies that collect and sell our data. In contrast, tools like Tor and I2P are designed to keep users anonymous. Interestingly, Tor was originally developed by the U.S. Navy for secure communication and later made public (Angelou & Veglis, 2024). Like a knife, the Dark-web can be used for both good and harm. The tool itself is not inherently bad; its impact depends on how people use it. This raises a difficult question: Should the Dark-web be banned because of its dangers, or protected because of its benefits? A complete ban might stop some crimes; but it could also silence the people who need it most. Instead, governments must strike a balance; target real criminals while protecting online freedom and privacy. Public education on safe internet use is also crucial. The Dark-web isn't just a place of darkness; it can also be a space of hope for those living in fear.

Future Research Directions

As technology continues to evolve, future research must explore how emerging tools like AI, deepfakes; and blockchain are changing the way the Dark-web is used. These technologies are making it easier to hide identities; create fake content, and build anonymous networks. At the

same time, tools for tracking and regulating cybercrime are also improving. Researchers need to study how this digital arms race is unfolding. Another important area is accessibility how people from rural areas or low-income backgrounds are entering the Dark-web; often without knowing the risks. Future studies should also look at how digital education, policy reforms; and cybersecurity training can help protect users while preserving freedom online. More attention is needed on how gender, caste, and class influence who is more vulnerable in hidden internet spaces. Exploring these issues will help create safer; and more inclusive digital futures.

Conclusion

The TOR network is a special system that helps people stay private online. It hides a user's location and browsing activity. This is helpful for people who want to avoid being watched. For example, people living in countries with strict rules can use TOR to speak freely. However, TOR is not perfect. It hides what you do online; but it does not hide the fact that you are using TOR. So, internet service providers (ISPs) can still tell that someone is using TOR, even if they cannot see what they are doing. TOR users can also change some settings to make their experience better. People who care more about privacy can choose options that make them more secure. Others who want faster speed may choose a different setup. So, the TOR browser gives people choices; depending on what they want. Besides TOR, there are other tools used on the Dark-web. One of them is called I2P. It stands for "Invisible Internet Project." Like TOR, I2P is also used to hide people's online activities. It sends messages through many computers so that no one knows where the message came from or where it is going. All traffic stays inside the I2P network. People use I2P to chat, share files, or visit hidden websites called "epistles." These sites have names ending in. i2p. I2P makes it harder for hackers or others to see who is talking to whom. Still, it has some problems. I2P is harder to set up than TOR. It also has fewer users, which means it can be easier to attack. Some past security problems have also affected I2P, so people need to be careful.

Another tool is called Freenet. Freenet is a software that lets people share files and information in a private way. It has been around for more than 20 years. Freenet works by sharing data across many users' computers. The data is cut into small pieces, and each user stores a few of these pieces. No user knows what the full data is or who sent it. This keeps things private. Freenet is often used to post articles, share documents, and have online discussions. But Freenet also has limits. Each computer can only store a small amount of data; and users do not know exactly what files they are sharing. Also, finding specific data on Freenet can be slow. Still, it is a useful tool for those who want free and open communication. All of these networks- TOR, I2P, and Freenet- try to give people more privacy online. They are helpful for journalists, activists, and others who need to stay safe. But they also come with risks. Not all people use them for good purposes. Some use them to hide bad or illegal actions. Because of this, these tools are often talked about in debates about internet safety and freedom. Cryptocurrencies are another important part of the Dark-web. These are digital money systems that do not need banks. Bitcoin was the first one, created in 2009 by a person (or group) using the name Satoshi Nakamoto. No one knows who this person really is. Bitcoin uses a special technology called blockchain. This is like a digital notebook that records every payment and cannot be changed easily. Other cryptocurrencies like Ethereum and Litecoin were created after Bitcoin. These digital coins can be used to pay for things on the Dark-web because they do not need names or bank accounts. That is why some people use them to stay hidden. Buying and using cryptocurrencies is not very hard today. People can use websites like Binance, Coinbase, or Crypto.com. First, you need to make an account and show your ID. Then you add money using a bank card or PayPal. After that, you can buy digital coins. But you need a safe place to keep them. You can store your coins on the same website where you bought them. Or you can move them to something called a "hot wallet" (which is online) or a "cold wallet" (which is offline, like a USB stick). Cold wallets are safer, but if you lose the password, you lose your money forever. In the end, technologies like TOR, I2P, Freenet, and cryptocurrencies help people stay private. They let people talk, share, and buy things without others watching. But with these tools, people must be careful. They can protect good people; but they can also be used for crime. So, using these tools in a smart and safe way is very important.

Acknowledgment

I sincerely thank my research supervisor, Dr. Keyoor Pathak (Assistant Professor, Department of Sociology, University of Allahabad), for his invaluable guidance. I also extend my heartfelt thanks to all my fellow research scholars.

References

1. Androulaki E., Karame G. O., Roeschlin M., Scherer T., & Capkun S. (2013). Evaluating user privacy in Bitcoin. In Sadeghi A. R. (Ed.), *Financial cryptography and data security. FC 2013. Lecture Notes in Computer Science*, (Vol. 7859, pp. 34–51). Springer. https://doi.org/10.1007/978-3-642-39884-1_4
2. Angelou, I., & Veglis, A. (2024). Greek legacy media organizations in the digital age: a historical perspective of web tool adoption (1990s–2023). *Internet Histories*, *8*(3), 229–245. https://doi.org/10.1080/24701475.2024.2303697
3. Badhwar R. (2021). Dark-web & dark net. In *The CISO's next frontier* (pp. 365–369). Springer International Publishing. https://doi.org/10.1007/978-3-030-75354-2_45
4. Bradshaw S., & Howard P. N. (2019). *The global disinformation order: 2019 Global inventory of organised social media manipulation* (Computational Propaganda Research Project). Oxford Internet Institute. https://comprop.oii.ox.ac.uk/research/

posts/the-global-disinformation-order-2019-global-inventory-of-organised-social-media-manipulation/#continue
5. Chaves, A. P., & Gerosa, M. A. (2020). How Should My Chatbot Interact? A Survey on Social Characteristics in Human–Chatbot Interaction Design. *International Journal of Human–Computer Interaction*, *37*(8), 729–758. https://doi.org/10.1080/10447318.2020.1841438
6. Chen X., Hasan M., Al Wu X., Skums P., Feizollahi M. J., Ouellet M., Sevigny E. L., Maimon D., & Wu Y. (2019). Characteristics of Bitcoin transactions on cryptomarkets. In Wang G., Feng J., Bhuiyan M., Lu R. (Eds.), *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, LNCS (Vol. 11611, pp. 261–276). https://doi.org/10.1007/978-3-030-24907-6_20
7. Chen, Z., Jardine, E., Fan Liu, X., & Zhu, J. J. H. (2022). Seeking anonymity on the Internet: The knowledge accumulation process and global usage of the Tor network. New Media & Society, 26(2), 1074-1095. https://doi.org/10.1177/14614448211072201
8. Collier, B. (2022). *TOR: From the Dark-web to the Future of Privacy*. The MIT Press.
9. Collier, B., & Stewart, J. (2021). Privacy Worlds: Exploring Values and Design in the Development of the Tor Anonymity Network. Science, Technology, & Human Values, 47(5), 910-936. https://doi.org/10.1177/01622439211039019
10. Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. The Police Journal, 96(4), 573-592. https://doi.org/10.1177/0032258X221107584
11. Davies, G. (2020). Shining a Light on Policing of the Dark-web: An Analysis of UK Investigatory Powers. The Journal of Criminal Law, 84(5), 407-426. https://doi.org/10.1177/0022018320952557
12. Dearden, T. E., & Tucker, S. E. (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
13. Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. Big Data & Society, 3(2). https://doi.org/10.1177/2053951716679678
14. Eklund, L., von Essen, E., Jonsson, F., & Johansson, M. (2021). Beyond a Dichotomous Understanding of Online Anonymity: Bridging the Macro and Micro Level. Sociological Research Online, 27(2), 486-503. https://doi.org/10.1177/13607804211019760
15. Frischlich L., Boberg S., & Quandt T. (2019). Comment sections as targets of dark participation? Journalists' evaluation and moderation of deviant user comments. *Journalism Studies*, 20(14), 2014-2033. https://doi.org/10.1080/1461670X.2018.1556320
16. Gadek, G., Brunessaux, S., & Pauchet, A. (2018). Applications of AI techniques to deep web social network analysis. *North Atlantic Treaty Organization Science and Technology Organization*: Semantic Scholar. Retrieved from. https://pdfs.semanticscholar.org/e6ca/0a09e923da7de315b2c0b146cdf00703e8d4.pdf
17. Gehl R. W. (2018). *Weaving the dark-web: legitimacy on freenet, Tor, and I2P*. MIT Press. https://doi.org/10.7551/mitpress/11266.001.0001
18. Gehl, R. W. (2014). Power/freedom on the dark-web: A digital ethnography of the Dark-web Social Network. New Media & Society, 18(7), 1219-1235. https://doi.org/10.1177/1461444814554900
19. Hegarty, K. (2025). Averting the Digital Dark Age: How Archivists, Librarians, and Technologists Built the Web a Memory: By Ian Milligan, Johns Hopkins University Press, 2024, 208 pp., ISBN 9781421450131. *Internet Histories*, 1–4. https://doi.org/10.1080/24701475.2025.2465221
20. Hiramoto N., & Tsuchiya Y. (2020). Measuring dark-web marketplaces via bitcoin transactions: From birth to independence. *Forensic Science International: Digital Investigation*, 35, 301086. https://doi.org/10.1016/j.fsidi.2020.301086
21. Howell, C. J., Fisher, T., Muniz, C. N., Maimon, D., & Rotzinger, Y. (2023). A Depiction and Classification of the Stolen Data Market Ecosystem and Comprising Darknet Markets: A Multidisciplinary Approach. Journal of Contemporary Criminal Justice, 39(2), 298-317. https://doi.org/10.1177/10439862231158005
22. Jenkins H., Ito M., boyd D. (2016). *Participatory culture in a networked era: A conversation on youth, learning, commerce, and politics*. Polity Press.
23. Jørgensen, R. F., & Desai, T. (2017). Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google. *Nordic Journal of Human Rights*, *35*(2), 106–126. https://doi.org/10.1080/18918131.2017.1314110
24. Koenraadt, R., & van de Ven, K. (2017). The Internet and lifestyle drugs: an analysis of demographic characteristics, methods, and motives of online purchasers of illicit lifestyle drugs in the Netherlands. *Drugs: Education, Prevention and Policy*, *25*(4), 345–355. https://doi.org/10.1080/09687637.2017.1369936
25. Kwon, K. H., Xu, W. W., & Wellman, B. (2021). The Dark Social Web: Responsibility, Manipulation, and Participation in Global Digital Spaces. American Behavioral Scientist, 65(5), 683-688. https://doi.org/10.1177/0002764221989782
26. Madouh, M., & Kwon, K. H. (2023). Evolving in the Shadows: A Media Ecology Study of Dark-web Social Networks. Journal of Communication Inquiry, 0(0). https://doi.org/10.1177/01968599231210776
27. Merrill, S. (2024). Remembering like a state: Surveillance databases, digital activist traces and the repressive potential of mediated prospective memory. Memory Studies, 17(5), 1177-1194. https://doi.org/10.1177/17506980241262187
28. Nearchou, N. (2023). *Combating Crime on the Dark-web*. Packt Publishing.
29. Ngo, F. T., Marcum, C., & Belshaw, S. (2023). The Dark-web: What Is It, How to Access It, and Why We Need to Study It. Journal of Contemporary Criminal Justice, 39(2), 160-166. https://doi.org/10.1177/10439862231159774
30. Papacharissi Z. (2015). *Affective publics: Sentiment, technology, and politics*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199999736.001.0001
31. Rainie L., & Wellman B. (2019). The internet in everyday life: the turn to networked individualism. In Graham M., Dutton W. (Eds.), *Society and the internet* (2nd ed., pp. 27-42). Oxford University Press. https://doi.org/10.1093/oso/9780198843498.003.0002
32. Sayyed, H., & Paul, S. R. (2025). Exploring the role of encryption and the dark-web in cyber terrorism: legal challenges and countermeasures in India. *Cogent Social Sciences*, *11*(1). https://doi.org/10.1080/23311886.2025.2479654
33. Schriner, J. (2019). Weaving the Dark-web: Legitimacy on Freenet, Tor, and I2P. *Internet Histories*, *3*(3–4), 388–390. https://doi.org/10.1080/24701475.2019.1623002
34. Swart J., Peters C., & Broersma M. (2018). Shedding light on the dark social: The connective role of news and journalism in social media communities. *New Media & Society*, 20(11), 4329-4345. https://doi.org/10.1177/1461444818772063
35. Warf, B. (2018). Internet origins and history. In The SAGE Encyclopaedia of the internet (Vol. 3, pp. 543-553). SAGE Publications, Inc., https://doi.org/10.4135/9781473960367.n155

HOW TO CITE THIS ARTICLE: Gond A.K. (2025). Hidden Side of the Internet: Between Crime and Freedom on the Dark-Web. *Journal of Communication and Management*, 4(3), 55-61. DOI: 10.58966/JCM2025436