Journal of Information Technology and Computing
https://jitc.sabapub.com
ISSN: 2709-5916

2025 Volume 5, Issue 1: 25–32
DOI: https://doi.org/10.48185/jitc.v5i1.1140

The Dark Web and The Digital Law, The Ongoing Battle Against Cybercrime

Raja Vavekanand*
[1] Department of Information Technology, Benazir Bhutto Shaheed University Lyari Karachi Sindh

Received: 06.04.2024 • Accepted: 20.07.2025 • Published: 14.09.2025 • Final Version: 12.10.2025

Abstract: The internet has become the basic need of the current generation. Utmost of the population around the world these days is using the internet regularly. The internet is a vast and intricate web of information, connecting billions of users worldwide. Within this web is a hidden layer known as the Dark Web, a space characterized by its anonymity and opacity. The Dark Web is a realm where the law finds itself at odds with a complex web of cybercriminal activities. The Dark Web, a subset of the Deep Web, is intentionally hidden from conventional search engines.

Keywords: Enter up to five keywords and separate them by commas

1. Introduction

The World Wide Web (www) is a complex system that consists of an unprecedented amount of digital information. The normal Internet used daily is accessible through standard search engines such as Google and Yahoo. However, there are large sections of the Internet that are unindexed and hidden from the normal search engines. This concealed part of the Internet is the Deep Web which is estimated to make up about 96 percent of the WWW. Within the Deep Web, a subset that is mostly used for illicit purposes is the Dark Web or the Dark Net. Criminal activities and illegal content are used with a percentage of 57% in the Dark Web.

These commonly include illegitimate drugs, weapons trafficking, child pornography, stolen financial details, unlawful discussions, fake currency, terrorist communication, and more. In 2013, when the US Federal Bureau of Investigation (FBI) shut down the most infamous marketplace Silk Road operating in the Dark Web, these criminal activities caught the attention of the public. Hidden wiki and Deep search engine way to browse malicious intents and illicit contents in the Dark Web. These sites provide links access to many other links in the Deep Web. One of the main obstacles the forensic analysts face while investigating the criminal's activity in the Dark Web is the anonymity presented in the Dark Web services. The contents and services provided by the Dark Web are commonly used by anonymous services such as Tor, Freenet, I2P, and Jon Donym. The most popular service in the Dark Web is the TOR network which provides the facility for the users to secretly share information anonymously via peer-to-peer connections instead of a centralized computer server.

1.1 Background Study

The internet has enabled the formation of a global digital society that transcends boundaries, be they nationalities, legal jurisdictions, race, or religion. This society, despite its amorphous nature, still

* Corresponding Author: *rajavavekanand@yahoo.com

constitutes individuals bound by the laws of their country. The Dark Web facilitates the sharing of arms and child pornography, providing encrypted anonymity for consumers. Numerous works of literature enhance the study, utilizing US intelligence systems for TOR routing. The Dark Network mechanism can be used for legitimate and illegal purposes, with privacy protection and ISI testing frameworks for data evaluation. The literature review provides a thorough analysis of the Dark Web and highlights important aspects of the researcher's study.

Barnett et al. study the function of spiders on the World Wide Web and their ease of access. Social network analysis (SNA) is used to evaluate network structure and population power. SNA methods are developed for analyzing forum posting and website connections, making it easier to collect necessary information.

Terrorism Informatics focuses on understanding remote networks and their characteristics, using coding systems to identify militant websites and terrorism content. Sensitivity and impact analysis detect violent sites, using specialized knowledge processing and methodologies from various fields.

1.2 The Deep Web and the Dark Web

1.2.1 The Deep Web

The deep web refers to all of the content on the internet that is not indexed by search engines like Google, Bing, or Yahoo. This means that you can't find these websites by simply typing in a keyword or phrase. The deep web is much larger than the surface web, which is the part of the internet that you can access through search engines. Estimates suggest that the deep web is 96-99% of the entire internet.

- Paywalled Content: This includes things like streaming services, online databases, and academic journals. You have to pay to access this content, so search engines can't crawl it.
- Private Accounts*:* Your bank account, email, and social media profiles are all part of the deep web because they require you to log in to access them.
- Dynamically Generated Content*:* This is content that is created on the fly when you interact with a website, such as the results you see on a search engine. Search engines can't index this content because it doesn't exist until you create it.

1.3.1 The Dark Web

The dark web is a hidden part of the internet hidden even within the vast Deep Web. Think of it as a secret tunnel within the iceberg from the previous analogy. Here's the lowdown:

- **Access:** Requires special software like Tor for anonymity.
- **Size:** Tiny, around 5% of the Deep Web (a fraction of the internet).
- **Content:** Mix of legitimate and illegal activities.
- **Legitimate**: Secure communication tools, alternative marketplaces, and whistleblower platforms.
- **Illegal:** Drug trafficking, cybercrime, stolen data, illegal pornography.
- **Risks:** High anonymity attracts both good and bad actors, so caution is crucial.

Characteristics	Deep Web	Dark Web
Basic	Deep web is a huge set of hidden websites whose matter is not a segment of Surface Web.	The Dark Web is a portion of Deep Web that's not synchronized and IP address are purposely concealed.
Access	It can be retrieved through an acceptable username or credentials and using common search engines.	It can only be retrieved with the help of specific software or where IP addresses are not locatable.
Involves	All pages that are not indexed.	It is a section of undirected pages within the deep web
Portion of Internet	It accounts for 96% of the internet	It accounts for 0.05% of the Internet.
Usage	It is used for legal activities that require privacy.	It may be used for either legal or illegal activities
Who utilizes it	Reporters, Informers, etc.	Dealers of illicit trade.

Figure 1: Difference between Deep Web and Dark Web

2. Dark Web as a Phenomenon

The dark web is a realm of the internet intentionally hidden from conventional search engines and only accessible through specialized software like Tor (The Onion Router). While it's often associated with illegal activities due to its anonymity features, the dark web itself is a broader phenomenon. It serves as a platform for privacy advocates, whistleblowers, and individuals seeking to bypass censorship in oppressive regimes.

On the flip side, the dark web has gained notoriety for hosting illicit marketplaces trading in drugs, hacking tools, and other illegal goods and services. It's essential to recognize the duality of the dark web as a space that both protects privacy and facilitates criminal activities. Understanding the dark web involves acknowledging its legitimate uses while addressing the challenges posed by illegal activities. As governments and cybersecurity experts grapple with regulating this hidden part of the internet, discussions around its impact on privacy, security, and freedom of information continue to evolve**.**

2.1 How Dark Web Works?

TOR websites are commonly used among the Dark Web users. TOR websites are addressed by the ".onion" domain. TOR browser focuses on providing mysterious access to the Dark Web on the Internet. Every website or web address denotes a node or starting point on the Dark Web.

- *Specialized Software:* Accessing the dark web typically requires using specialized software like Tor (The Onion Router). Tor anonymizes internet traffic by bouncing it through a network of volunteer-operated servers, encrypting the data and making it difficult to trace back to the user.
- *Onion Routing:* Tor uses a technique called onion routing, where data is encrypted in layers (like the layers of an onion). Each server in the network peels off one layer, revealing the instructions to reach the next server. This process repeats until the final server decrypts the data and sends it to its destination.
- *Onion Domains:* Websites on the dark web often use ".onion" domains instead of traditional top-level domains (e.g., .com or .org). These domains are not indexed by standard search engines and can only be accessed through Tor.
- *Enhanced Privacy*: Users on the dark web can maintain a higher level of privacy compared to the surface web. This anonymity attracts individuals seeking privacy for legitimate reasons, such as activists, journalists, or citizens in oppressive regimes. However, it also facilitates illegal activities.
- *Decentralized Nature:* The dark web is decentralized, making it resistant to censorship. Since there is no central authority controlling access, it is challenging for governments or other entities to shut it down entirely.

2.2 Accessing Dark Web

Accessing the dark web involves specific steps to ensure privacy and anonymity. However, it's important to note that engaging in illegal activities on the dark web is against the law. Here's a general guide for educational purposes only:

Download and Install the Tor Browser: Obtain the Tor Browser from the official Tor Project website.

- *Configure Tor Browser:* Open the Tor Browser and follow the setup instructions, Adjust security settings as needed, but be aware that higher security levels might limit some functionalities.
- *Access .onion Websites:* Use the Tor Browser to visit websites with ".onion" domains, which are specific to the dark web, Search for directories and forums that list .onion sites, as conventional search engines won't index them.
- *Exercise Caution:* Be extremely cautious about the sites you visit. The dark web harbors illegal activities and accessing certain content may have legal consequences.
- *Prioritize Privacy:* Disable JavaScript to enhance privacy, but be aware that some sites may not function properly without it, Consider using a VPN (Virtual Private Network) in addition to Tor for an extra layer of anonymity.
- *Understand Risks and Legal Implications:* Be aware of the potential risks associated with accessing the dark web, including exposure to illegal content, scams, and cyber threats. Understand the legal implications in your jurisdiction, as accessing certain content may violate the law.

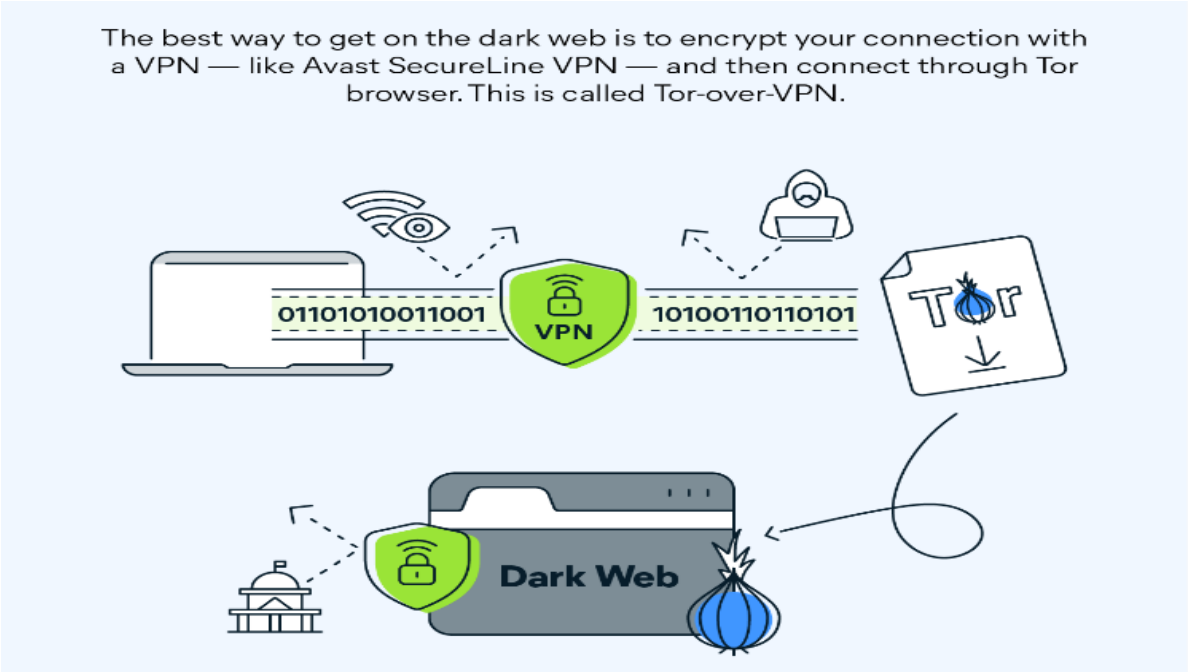

Figure 2: Accessing Dark Web

3. Cybercrime in the Dark Web

The dark Web is the portion of the deep Web that has been intentionally hidden and is inaccessible through standard Web browsers. Dark Web sites serve as a platform for Internet users for whom anonymity is essential since they not only provide protection from unauthorized users but also usually include encryption to prevent monitoring. A relatively known source for content that resides on the dark Web is found in the Tor network.

The Dark Web hosts a wide range of illegal activities, facilitated by the cloak of anonymity it provides. These activities are often divided into various categories, each with its own set of challenges for law enforcement.

- *Black Markets and Contraband Trade:* The Dark Web is infamous for its black markets, where virtually anything can be bought and sold. This includes illegal drugs, firearms, stolen data, counterfeit currency, and more. The Silk Road, a prominent black market, gained notoriety before law enforcement shut it down.
- *Hacking and Data Breaches:* The Dark Web offers a haven for skilled hackers for hire. These hackers exploit vulnerabilities, steal sensitive data, and launch attacks on organizations. Such breaches can lead to significant financial losses, identity theft, and company reputation damage.
- *Cyberattacks for Hire:* Criminals on the Dark Web offer their services to the highest bidder. This includes launching distributed denial of service (DDoS) attacks, ransomware attacks, and espionage activities, often for economic or political motives.
- *Online Fraud:* The Dark Web frequently orchestrates credit card fraud, identity theft, and phishing schemes. Criminals can buy or sell stolen financial information with relative ease, leading to substantial financial losses for victims.

- *Malware and Exploits:* The Dark Web is a marketplace for malicious software, including ransomware, trojans, and zero-day vulnerabilities. This fuels the spread of malware, allowing cybercriminals to infiltrate systems and steal valuable data.

Figure 3: Dark Web marketplaces offer a variety of illegal goods for sale

4. Digital Law Enforcement

Digital law enforcement agencies employ various strategies to combat illegal activities on the dark web, where criminal enterprises often thrive. These efforts aim to enhance cybersecurity, protect users, and curb illicit transactions**.**

4.1 Challenges of Policing the Dark Web

Anonymity: The dark web's core strength lies in its anonymity. Users rely on encrypted communication channels and masked IP addresses, making it difficult to track their activity and identify them.

Encryption: Strong encryption protocols further impede investigations. Cracking these codes requires advanced technical expertise and often legal hurdles.

Jurisdictional Issues: Criminal activity on the dark web often transcends national borders, making it challenging for law enforcement agencies to coordinate investigations and prosecutions.

Rapidly Evolving Landscape: Dark web marketplaces and forums constantly change tactics and adapt to new technologies, making it difficult for law enforcement to keep pace.

Strategies for Combating Dark Web Crime

Infiltration and Undercover Operations: Specially trained officers pose as buyers or sellers to infiltrate criminal networks, gather evidence, and identify key players.

Data Analysis and Tracing: Advanced data analysis tools help track cryptocurrency transactions, analyze communication patterns, and identify potential illegal activity.

International Cooperation: Law enforcement agencies around the world are increasingly collaborating to share information, coordinate investigations, and dismantle criminal organizations.

Public Awareness and Education: Raising public awareness about the dangers of the dark web and educating users on safe online practices can help prevent victimization.

4.2 Successful Operations

Operation Dark Market: A global sting operation in 2021 shut down the world's largest illegal marketplace on the dark web, leading to the arrest of 54 people and the seizure of millions of euros in cryptocurrency.

Operation Onymous: A joint effort by Europol and several national law enforcement agencies led to the takedown of the AlphaBay market, another major dark web marketplace, in 2022.

4.3 Technological Advancements

Law enforcement agencies are constantly investing in new technologies to improve their ability to combat dark web crime.

- *Artificial intelligence (AI):* AI-powered tools can analyze vast amounts of data to identify suspicious activity and patterns.
- *Blockchain Forensics:* Tracking cryptocurrency transactions on the blockchain can help identify criminals and their financial networks.
- *Zero-Day Exploits:* Law enforcement agencies may use zero-day exploits, vulnerabilities unknown to the public, to gain access to encrypted dark web communications.

4.4 The Future of Digital Law Enforcement

The battle against dark web crime is an ongoing one. As criminals continue to adapt and develop new technologies, law enforcement agencies must constantly evolve their strategies and tools. International cooperation, technological advancements, and public awareness will be crucial in this fight to make the dark web a safer place.

It's important to remember that while the dark web presents significant challenges, law enforcement agencies are making strides in combating the illegal activities that take place there. With continued investment in technology, collaboration, and education, we can make the Internet a safer place for everyone.

5. Conclusion

The dark web, due to its anonymity, struggles to distinguish between malicious and authentic users. Enforcement authorities must implement techniques to protect user privacy and catch criminals. Investigating fraudulent sites can be an efficient way to tackle this issue. Surfing the dark web is not illegal, but engaging in illegal activities is wrong. Ethical hackers can install deanonymizing tools in users' systems, and enforcers can force charges against mischievous site authors. Breaking Tor, identifying every Tor user, could create a more robust service and destroy useful tools like dissidents for authentic users. The anonymity of online users is a double-edged sword, requiring vigilant monitoring and legal support to successfully police the dark web. As policymakers progress, more vigilant monitoring and enforcement authorities are needed to ensure the safety and security of the dark web.

References

[1] Hurlburt, G. (2017). Shining Light on the Dark Web. Computer, 50(4), 100–105. doi: 10.1109/mc.2017.110

[2] Bradbury, D. (2019, January 6). Silk Road and Beyond: Bitcoin's Complex Relationship With the Dark Web. Retrieved from https://www.thebalance.com/what-is-a-dark-market- 391289

[3] A public policy perspective of the Dark Web. (n.d.). Retrieved from https://www.tandfonline.com/doi/full/10.1080/23738871.2017.129864 3

[4] What is the Difference Between the Surface Web, the Deep Web, and the Dark Web? (2018, October 11). Retrieved from https://resources.infosecinstitute.com/what-is-the- difference-betweenthe-surface-web-the-deep-web-and-the-dark-web/#gref

[5] https://www.avast.com/c-dark-web

[6] Palash Goyal, KSM Hossain, Ashok Deb, Nazgol Tavabi, Nathan Bartley, Andr'es Abeliuk, Emilio Ferrara, and Kristina Lerman. 2018. Discovering Signals from Web Sources to Predict Cyber Attacks. arXiv preprint arXiv:1806.03342 (2018).

[7] Thomas L Griffiths, Mark Steyvers, David M Blei, and Joshua B Tenenbaum. 2005. Integrating topics and syntax. In NIPS. 537–544.

[8] Amit Gruber, Yair Weiss, and Michal Rosen-Zvi. 2007. Hidden topic markov models. In Artificial intelligence and statistics. 163–170.

[9] Nils Lid Hjort et al. 1990. Nonparametric Bayes estimators based on beta processes in models for life history data. The Annals of Statistics 18, 3 (1990), 1259–1294.

[10] Matthew Honnibal and Ines Montani. 2017. spaCy 2: Natural language understanding with Bloom embeddings, convolutional neural networks, and incremental parsing. (2017).

[11] George Hurlburt. 2017. Shining Light on the Dark Web. IEEE Computer 50, 4 (2017), 100–105. Sharma, M., Tandon, A., Narayan, S., & Bhushan, B. (2017).

[12] Classification and analysis of security attacks in WSNs and IEEE 802.15.4 standards: A survey. 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA).

[13] Biswas, R., Fidalgo, E., & Alegre, E. (2017). Recognition of service domains on the TOR dark net using perceptual hashing and image classification techniques. 8th International Conference on Imaging for Crime Detection and Prevention (ICDP 2017). doi: 10.1049/ic.2017.0041

[14] Singh, A., Sharma, A., Sharma, N., Kaushik, I., & Bhushan, B. (2019). Taxonomy of Attacks on Web-Based Applications. 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT).

[15] East, C. S. (2017). Demystifying the Dark Web. Itnow, 59(1), 16–17. doi: 10.1093/itnow/bwx007

[16] What's the Dark Web & How to Access It in 3 Easy Steps - 2020. (n.d.). Retrieved from https://www.vpnmentor.com/blog/whats-thedark-web-how-to-access-it-in-3-easy-steps/

[17] Bradbury, D. (2019, January 6). Silk Road and Beyond: Bitcoin's Complex Relationship With the Dark Web. Retrieved from https://www.thebalance.com/what-is-a-dark-market- 391289.