COMPUTOLOGY: Journal of Applied Computer Science and Intelligent Technologies
Volume 2, Issue 1, Jan-Jun 2022, pp. 44-52
DOI: 10.17492/computology.v2i1.2206
https://www.journalpressindia.com/cjacsit

Dark Web: A Playground for Cyber Criminals

*Keshav Kaushik**

ABSTRACT

So far as we know, DarkWeb Crimes is one of the more sophisticated organised cybercrimes that not many people are aware of. DarkWeb is a haven for international criminals. It may not be simple to define what DarkWeb is. The primary entry point to the dark web (TOR) is the Tor network, commonly referred to as The Onion Router. The word comes from the idea that the numerous layers of an onion symbolise the various levels of anonymity and secrecy available on the dark web. The technology found on the Darknet is not limited to a particular platform or location. The Darknet saw a surge in several crimes, including as the sale of illegal substances, financial fraud, counterfeit money, data breaches, the sale of forged passports, viral forums, child pornography, and other unlawful activities. The author of this essay has covered the many types of cybercrimes that occur on the dark web. The writers have provided instructions on how to enter the dark web and take advantage of many individuals.

Keywords: Dark Web; Deep Web; Cybercrimes; Cyber frauds; Cyberspace; Cybersecurity.

1.0 Introduction

Unprecedented technological developments brought about by the digital era have connected people worldwide like never before. But this connectivity has also resulted in the emergence of the Dark Web, a parallel, mysterious, and frequently malicious domain. For the great majority of internet users, this hidden aspect of the internet is still an enigmatic mystery. The Dark Web is home to a secretive ecosystem that is thriving on secrecy, anonymity, and criminality; it is a virtual playground for cybercriminals, hidden away in its shadowy corners. The idea of the "Dark Web" is difficult to define. It functions beyond Surface Web's apparent boundaries, which are the websites that can be found using conventional search engines like Google. Rather, specialised browsers such as Tor (The Onion Router) are required to access the Dark Web. The acronym "Tor" is a fitting representation of the layers of obfuscation and encryption that envelop its inhabitants in an almost impermeable obscurity.

This paper begins a thorough investigation of the Dark Web, revealing its mysteries and illuminating the murky activities that take place within its virtual walls. From its beginnings as a safe refuge for political dissidents, privacy-conscious people, and whistleblowers, the Dark Web has experienced a radical transformation. It has developed into a bustling market for illicit products and services, a haven for cybercriminal syndicates, and a haven for people looking to use the internet [1] for evil. We explore the many facets of Dark Web crimes in this talk, including the illegal drug trade, financial fraud schemes, the spread of counterfeit money, massive data breaches, the nefarious trade in fake passports, the spread of malicious forums, and the abhorrent distribution of child pornography.

**School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India (E-mail: officialkeshavkaushik@gmail.com)*

Every aspect of this shadowy realm is closely scrutinised, offering a comprehensive comprehension of the extent and severity of cybercrime operations that afflict the Dark Web.

We also provide a practical analysis of the tools and techniques that cybercriminals use to get access to and prosper in this underground economy. Although there is no denying the Dark Web's attraction and anonymity potential, it is important to emphasise the hazards and ethical issues that come with navigating these unexplored digital seas. We encourage readers to investigate the internet's underbelly and peek behind the curtain as we set out on our adventure into the depths of the Dark online. our world stands in sharp contrast to the open and interconnected online that we use daily. We hope to demystify the Dark Web, sort out its intricacies, and illuminate the frightening reality that it has turned into—a virtual haven for cybercriminals—through our investigation.

Each of the three levels of the internet—the Surface Web, the Deep Web, and the Dark Web—has its own specific features.

- Exposed Network: The Surface Web [2] is the part of the internet that can be accessed publicly using well-known search engines such as Google, Bing, and Yahoo. Content Accessibility: All Surface Web sites are crawled and searchable by anybody. Websites including news sites, social networking hubs, and online stores are all included here. Since the identities of website owners are generally known and controlled, information on the Surface Web is transparent.
- Dark Web: The Deep Web is a term used to describe the portion of the internet that is inaccessible by standard browsing and search engines. Content that requires payment, access to a database, participation in a secret forum, or use of a password is included. Authentication: Usually, you'll need some sort of authentication to see anything on the Deep Web, such a login and password or subscription credentials. Academic databases, medical records, and exclusive business information are just some of the treasures that may be found on the Deep Web, which is far more extensive than the Surface Web.
- Internet underworld: Hidden and anonymous, the Dark Web is a subset of the internet that has been designed to be out of the public eye. The Tor Browser or other such specialised software is required to access it. Users on the Dark Web can remain anonymous, and their data is encrypted to a great degree. Because data travels across a distributed system of "nodes," monitoring individual actions is next to impossible. Selling narcotics, guns, and stolen information are just a few of the many criminal activities that have made the Dark Web notorious. There are several hacker communities and networks based there as well.

2.0 The Secretive Appeal of the Deep Web

There is no denying the Dark Web's attraction and mystery, which piques the interest of many. Individuals who wish to conceal their online activity from prying eyes or government restrictions are drawn to the anonymity the Dark Web provides. Both the website's visitors and its administrators can surf in complete secrecy. Mysteriousness: People are intrigued by the Dark Web because of its hidden, encrypted nature. It's a haven for people or organisations who want to do their work without drawing attention from authorities. Information That Should Be Kept Secret: The Dark Web has long been linked to taboo subject matter. It houses underground wikis, message boards, and libraries that offer access to content that may be illegal or otherwise difficult to obtain on the Surface Web.

As a kind of "counter-censorship," the Dark Web is becoming important in countries where free speech online is restricted by authoritarian governments. This paper's goal is to educate readers on the Dark Web, all its nuances, and its relevance in the worlds of criminality and online anonymity. This

paper explores the architecture, practices, and underlying technology of the Dark Web to provide light on the following fundamental issues:

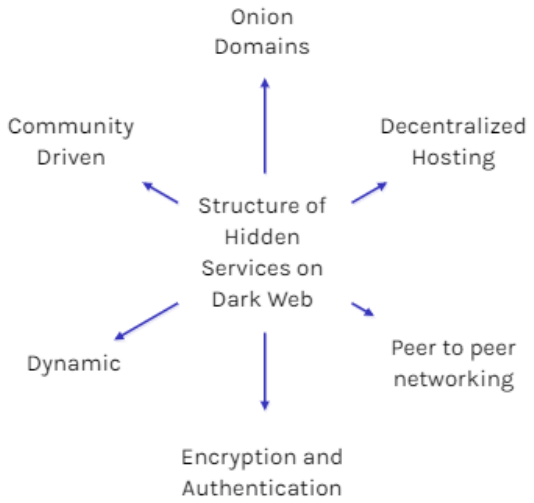
- The development and expansion of illicit activity on the Dark Web.
- What makes the Dark Web possible are the technology and instruments that make it work.
- An examination of the many forms of illegal activity and cybercrime that may be found on the Deep Web.
- Methods used by the government and the private sector to tackle criminality on the Dark Web are analysed.
- understanding of the Dark Web's future developments and patterns.

This paper's overarching goal is to clarify the Dark Web by showcasing its significant effects on the Internet, on cybersecurity, and on society at large. It encourages users to take a responsible and ethical approach to comprehending the Dark Web's complexities while serving as a thorough resource for navigating the Dark Web's intricate, secretive realm.

3.0 The Structure of Hidden Services (Websites)

The Dark Web functions as a covert subterranean network that is not visible to traditional web browsers or search engines. Figure 1 shows the structure of hidden services on dark web.

Fig 1: Structure of Hidden Services on Dark Web



What sets the Dark Web apart from the Surface Web is that it is primarily based on a special architecture called hidden services.

- Onion domains stand at the core of the hidden services hierarchy; they are domains ending in ".onion" rather than the more common ".com" or ".org." A sophisticated cryptographic procedure is used to produce these domains, producing a random alphanumeric string that is followed by ".onion." An example of a typical URL for a Dark Web website might be "examplewebsite.onion." These domains are an essential part of the Dark Web's anonymity since they are intended to be difficult to remember and difficult to monitor.
- Decentralised Hosting: Hidden services on the Dark Web are hosted in a decentralised fashion, in contrast to standard websites, which are housed on centralised servers with identifiable IP

addresses. This indicates that the server running a specific hidden service is purposefully concealed from view. The website's content is dispersed throughout a network of volunteer-operated nodes rather than depending on a single server, adding levels of security and anonymity.

- Peer-to-peer Networking: The Dark Web's hidden services are primarily supported by the Tor network, also known as The Onion Router. Before a user's request reaches the server hosting the hidden service, it is routed via an entrance node, middle node, and exit node among other Tor nodes when they visit a website with the ".onion" extension. By obscuring the user's IP address at every stage, this routing guarantees the preservation of their anonymity.
- Encryption and Authentication: To further improve security, user and hidden service communications are encrypted. Users' device and the website's server create a secure connection using encryption methods when they visit a hidden service. In addition to protecting the communication's content, this encryption confirms the legitimacy of the concealed service, lowering the possibility of phishing or spoofing attempts.
- Dynamic and Changing: The Dark Web's secret services have a dynamic, constantly changing structure. Because websites can come and go at any time, it can be difficult for law authorities to find and capture hackers. These websites' content, which may include everything from blogs and repositories to forums and markets, is likewise dynamic.
- Community-Driven: On the Dark Web, close-knit communities are frequently the lifeblood of hidden services. Many of these sites are only accessible with insider information or through referrals from other reliable users. This exclusivity acts as a barrier to admission for those who are unfamiliar with the Dark Web while also contributing to its mystery.

Gaining an understanding of the structure of hidden services is essential to appreciating the distinctive features of the Dark Web. Because of its organisational design, the Dark Web may operate as a place of anonymity and secrecy where cybercriminals can carry out illegal acts outside the purview of conventional law enforcement. However, because it evades common monitoring and identifying techniques, this structure also presents a huge barrier to efforts to curb Dark Web crime.

4.0 Getting into the Hidden Web

The Dark Web is a part of the internet that is not accessible through regular means, such as search engines or web browsers, and is therefore cloaked in mystery. A thorough familiarity with the underlying technology and a dedication to protecting one's privacy are essential for secure and efficient Dark Web access. Accessing the Dark Web safely is discussed here, as is the use of specialised browsers like the Tor Browser, and some of the more widespread misunderstandings that surround it.

4.1 Tips for protected use of the hidden internet

Create a Safe and Separate Space Before exploring the Dark Web, it's important to set up a safe and separate space on your device. This can be done by accessing the Dark Web via a special machine or a virtual machine (VM). Doing so reduces the likelihood that your primary device may be compromised.

- Install an OS Made for Privacy: If you're concerned about your privacy, you may want to install an OS made for privacy, such as Tails (The Amnesic Incognito Live System). Running Tails via a removable USB device ensures that no traces of the programme are left behind.

- To safely surf the Dark Web, the most popular tool is the Tor Browser, which can be downloaded for free. The Onion Router, or Tor, is the foundational network. Tor is a network of volunteer-operated relays that makes it extremely difficult to track your online activities.
- Acquaint yourself with the Tor Browser's configuration options to increase your anonymity. Potential security concerns can be reduced by adjusting security settings, customising privacy settings, and turning off JavaScript.
- The Tor browser is required for accessing ".onion" websites, which are found on the Dark Web. Standard web browsers are unable to access these Dark Web domains. Avoid suspicious connections and stick to sites recommended by trusted authorities.
- Good OpSec (Operational Security) dictates that you do not broadcast your identity or location while surfing the Dark Web. Avoid downloading files from the internet or visiting websites without first verifying their safety.
- Keep Your Software Up to Date Always keep your Tor browser, operating system, and security software up to date to guard against security flaws and new threats [3] [4].

4.2 The importance of unique web browsers (like Tor)

When accessing the Dark Web safely, the Tor Browser is crucial. It encrypts data as it travels via a network of user-operated servers, keeping your online activity private. Here are a few highlights of using the Tor Browser:

- The fundamental purpose of the Tor Browser is to conceal your online identity. It hides your IP address so that websites and other people can't determine where you are.
- The Tor Browser has built-in security measures including NoScript, which turns off JavaScript by default and reduces vulnerability to malicious scripts on websites.
- Tor Browser's interface was created with the average user in mind, making it simple to use even for individuals without any prior experience with computers.
- Developers constantly provide updates to fix security issues and enhance the system's performance.

4.3 Misconceptions about using Tor to access the dark web

Accessing the Dark Web does not necessarily equate to engaging in criminal activity, even though it does house unlawful activities. There are several perfectly valid uses for the Dark Web, such as user privacy, research, and unfiltered content. While Tor does a good job at hiding your IP address, it is not 100% secure. Your identity and whereabouts may be at risk if you made a few simple blunders. As a result, users need to be wary and adhere to safe browsing practises. Having criminal intent is not the same thing as having access to the Dark Web. To access resources under oppressive regimes, communicate securely, or circumvent internet restrictions are all valid uses. A mix of technological know-how, privacy tools like the Tor Browser, and a commitment to responsible online behaviour is necessary for secure access to the Dark Web. Anyone thinking about exploring the Dark Web must first dispel popular myths and learn the intricacies of accessing this secret part of the internet.

4.4 Contraband markets

It's well knowledge that the Dark Web is home to several underground markets where users may purchase and sell all manner of illegal goods and services. Here, we'll dig into the murky world of underground markets, describing the services and goods sold on such sites as Silk Road and AlphaBay, and addressing the efforts of government enforcement to shut them down.

Table 1: Comparison Analysis of Famous Dark Web Markets

Aspect	Silk Road	AlphaBay
Founding Year	2011	Estimated in 2014
Founder	Ross Ulbricht (Dread Pirate Roberts)	Alexandre Cazes (Alpha02)
Primary Focus	Illegal drug trade	Wide range of illicit goods and services
Notable Features	- Strict code of conduct - Emphasis on harm reduction - User-friendly interface	- Escrow system for secure transactions - Administrator monitoring - Extensive product listings
Shutdown and Arrests	Shut down in 2013, Ross Ulbricht arrested and sentenced to life in prison	Taken down in 2017, Alexandre Cazes arrested (died in custody)
Size and Popularity	Considered the first major Dark Web marketplace, gained significant media attention	One of the largest Dark Web marketplaces, attracted a large user base
Products and Services	Predominantly focused on drug trade, various types of narcotics	Diverse offerings, including drugs, firearms, hacking tools, counterfeit currency, and more
Reputation	Notorious for pioneering the Dark Web drug trade, garnered significant notoriety	Known for its extensive product listings and user-friendly features
Impact	Played a significant role in popularizing Dark Web marketplaces	Highlighted the challenges of combating large-scale Dark Web operations

5.0 List of Available Goods and Services

Figure 2 shows the prominent goods and services present on the dark web.

Figure 2: Prominent Goods and Services on Dark Web

- Drugs: Various illegal substances, legal treatments, and even high-end designer drugs can all be found for sale on dark web marketplaces. There are extensive descriptions of products, user reviews, and even vendor ratings available to consumers.
- Data Theft: Credit card details, login credentials, Social Security numbers, and even copies of personal papers have all been seen for sale by cybercriminals on the Dark Web. Identity theft and other forms of financial fraud are possible with this information.
- Arms and ammunition: The selling of weapons, ammunition, and weapon accessories is facilitated illegally by several Dark Web markets. These postings aren't as common as drug ads, but they nevertheless pose a risk because of their potential for abuse.

- Hacking Equipment: Cybercriminals go to the Dark Web in search of hacking tools, exploit kits, and unpatched programmes. Cyberattacks, data breaches, and unauthorised system access are all possible with the help of the objects.
- Currency counterfeiting: It is possible to buy counterfeit banknotes and coins on some online markets. The economic system is in danger because of these fake goods.

6.0 Efforts by Law Enforcement to Prevent Market Closures

Globally, law enforcement organisations have been working to eliminate unlawful Dark Web marketplaces and prosecute their administrators. These actions consist of:

- To obtain evidence against the merchants and operators of a market, law enforcement often sends in undercover officers.
- The takeover of the servers and infrastructure supporting these markets through concerted measures renders them inaccessible to users.
- Significant convictions and sentences have resulted from the arrest and prosecution of marketplace owners, administrators, and important sellers.
- Global Teamwork: International cooperation is commonplace in the dark web's marketplaces. Worldwide, law enforcement agencies are working together to identify and capture criminals.
- Authorities use asset forfeiture to seize money and other valuables associated with those who run black market websites.

Despite the triumphs of law enforcement, Dark Web markets persist. The continuous cat-and-mouse game between law enforcement and cybercriminals on the Dark Web's seedier side exemplifies the difficulty of putting a stop to illegal operations on the Deep Web.

7.0 Future of the Deep Web

Several new developments are influencing the future of the Dark Web:

- The Dark Web is not a fixed entity; rather, it evolves in response to new tools and increased scrutiny from authorities. The Dark Web will likely adapt and improve in the future.
- As more anonymity and encryption tools [5] become available, it will become increasingly difficult to detect and trace users of the Dark Web. For this reason, it may be necessary to adopt more secure alternatives to Tor, such as blockchain technology.
- Criminals engaging in cybercrime [6] may alter their methods in response to increased law enforcement pressure. This may need the implementation of decentralised, peer-to-peer networks, or the use of new coins that boast improved anonymity.

Security Measures for the Dark Web

- Individuals and businesses alike should familiarise themselves with the dangers of the Dark Web through education and awareness campaigns. The first step in protecting yourself from harm is realising what those dangers could be.
- Adopt stringent cybersecurity procedures, such as multiple factors of authentication, frequent software upgrades, and network monitoring to identify unusual activities.
- Organisations should give cybersecurity training to their staff so that they can identify and avoid phishing efforts and other forms of cybercrime that originate on the Dark Web.

- Tools for Anonymity and Privacy The use of trusted anonymity tools and virtual private networks (VPNs) can provide an additional layer of protection for users concerned about their online privacy.

Efforts to Regulate the Dark Web [7] to Reduce Illicit Activities

- To successfully tackle Dark Web operations, governments and law enforcement agencies throughout the world must unite. Cybercrime [8] does not respect national boundaries, thus fighting it requires cooperation.
- It is critical that laws be drafted and enforced that penalise conduct on the Dark Web. Legislation pertaining to the distribution of contraband, the disclosure of private information, and the misuse of virtual currencies is included in this category.
- Law enforcement organisations should keep an eye out for and shut down illicit Dark Web markets, as well as disrupt cybercriminal networks and apprehend those who are part of them.

Research on the Dark Web: Ethical Considerations

- Researchers have a need to act ethically when exploring the Dark Web. This includes abstaining from any illegal behaviour, protecting the privacy of Dark Web users, and gaining their informed consent before engaging in any kind of interaction with them.
- Carefully handle any information acquired from the Dark Web and use it solely for lawful academic inquiry.
- Scientists should make protecting people and the community their top priority. This includes keeping secrets that hackers may use against you.
- Clearly state your research's methodologies and aims. This assures ethical behaviour and helps keep the research community trusting.

The ever-evolving nature of the Dark Web presents both threats and possibilities. Effective mitigation methods, respectable research practises, and knowledge of developing trends are all necessary for traversing the Dark Web.

8.0 Conclusion

The Dark Web is still a mysterious and ever-evolving part of the internet because of its complex obscurity, developing technology, and cybercriminal underbelly. This section has explored its hidden architecture, shed light on its mysterious attraction, and analysed the wide variety of illegal activities that flourish within its virtual walls. Emerging anonymity trends and possible shifts in cybercriminal operations await as the Dark Web continues to impact the future of the digital world. Strategies for individual and institutional security, as well as international attempts at regulation, are required for ethical navigation of this murky space. To ensure that as we unravel its mysteries, we do so with honesty and dedication to minimising harm in our linked world, ethical issues in Dark Web study must stay at the forefront of scholarly investigation.

References

1. A. S. Beshiri, A. Susuri, A. S. Beshiri, and A. Susuri, “Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review,” *Journal of Computer and Communications*, vol. 07, no. 03, pp. 30–43, Mar. 2019, doi: 10.4236/JCC.2019.73004.

2. S. Kaur and S. Randhawa, "Dark Web: A Web of Crimes," *Wirel Pers Commun*, vol. 112, no. 4, pp. 2131–2158, Jun. 2020, doi: 10.1007/S11277-020-07143-2/METRICS.
3. R. Basheer and B. Alkhatib, "Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence," *Journal of Computer Networks and Communications*, vol. 2021, 2021, doi: 10.1155/2021/1302999.
4. S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan, "Evolution of dark web threat analysis and detection: A systematic approach," *IEEE Access*, vol. 8, pp. 171796–171819, 2020, doi: 10.1109/ACCESS.2020.3024198.
5. P. William, M. A. Jawale, A. B. Pawar, R. R. Bibave, and P. Narode, "Systematic Approach for Detection and Assessment of Dark Web Threat Evolution," *Using Computational Intelligence for the Dark Web and Illicit Behavior Detection*, pp. 230–256, Jan. 1AD, doi: 10.4018/978-1-6684-6444-1.CH013.
6. B. J. Holland, "Transnational Cybercrime: The Dark Web," *Encyclopedia of Criminal Activities and the Deep Web*, pp. 108–128, Jan. 1AD, doi: 10.4018/978-1-5225-9715-5.CH007.
7. K. Godawatte, M. Raza, M. Murtaza, and A. Saeed, "Dark web along with the dark web marketing and surveillance," *Proceedings - 2019 20th International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT 2019*, pp. 483–485, Dec. 2019, doi: 10.1109/PDCAT46702.2019.00095.
8. K. Kaushik, S. Tayal, A. Bhardwaj, and M. Kumar, "Advanced Smart Computing Technologies in Cybersecurity and Forensics," *Advanced Smart Computing Technologies in Cybersecurity and Forensics*, Nov. 2021, doi: 10.1201/9781003140023/advanced-smart-computing-technologies-cybersecurity-forensics-keshav-kaushik-shubham-tayal-akashdeep-bhardwaj-manoj-kumar.