

Cyber Crimes on Dark Web: The Digital Underground

Dr. Omkar Sonawane*

Independent Researcher.

*Corresponding Author: dromkarphd@gmail.com

Citation: Sonawane, O. (2026). Cyber Crimes on Dark Web: The Digital Underground. International Journal of Global Research Innovations & Technology, 04(03), 243–247. <https://doi.org/10.62823/ijgrit/04.03.9566>

ABSTRACT

The dark web represents a concealed segment of the internet that operates through anonymity-enhancing technologies, enabling users to communicate and exchange information beyond the reach of conventional search engines. While it serves the purpose of protecting privacy, secure communication, supports freedom of expression and share information. The dark web is now associated with cybercrime and criminal activities. Its anonymous nature has fostered the growth of illicit activities online, which include; illegal marketplaces, money laundering, cybercrime-as-a-service, ransomware-as-a-service, fraud operations, identity theft and distribution of malicious software. Cryptocurrencies have enabled these underground systems through digital payments, enabling anonymous financial transactions across cyberspace. The following paper aims to explore the dark web, its dynamic ecosystem that leads to organized cybercrime in cyberspace.

Keywords: Cybercrime, Cyber Space, Dark Web, Anonymity, National Security, Technology.

Introduction

Cyberspace today has become a zone of transition from the physical world to a virtual world. With heavy reliance on technology, it can be said that the internet has now generated innumerable risks online. It has allowed cybercriminals and criminal organizations to break geographical barriers and spread its tentacles to increase its reach and scale to commit cybercrimes, wherein computer systems have become their primary targets. Cybercrime today encompasses almost all areas of society and has affected people of all ages, leaving victims helpless, hopeless, worried, anxious, and vulnerable. Cybercrimes, which have been significantly increasing compared to traditional crimes, is now estimated to be in billions of dollars. The misuse of technology to commit crimes has become exponential, thus posing grave risks to cyberspace and national security. Debates on cybersecurity, particularly in the internet domain, mention that the dark web requires an integrated and transnational response, along with the need to associate its linkages to cyberspace and cybersecurity.

Dark Web¹ is a subset of deep web, which is an anonymous part of the web and can be accessed via Tor technology. Due to its anonymous nature, it has evoked many illegal activities online, which includes; drugs trafficking, human trafficking, weapon trafficking, illegal pharmaceutical, money laundering, whistleblowing, intelligence gathering, spyware², malware, identity theft stolen goods, exploit toolkits, phishing, remote access trojans, ransomware-as-a-service, cybercrime-as-a-service, ddos-as-a-service, and anonymous chat forums. The anonymity provided by the dark web is what makes it attractive to cybercriminals, which has now become the preferred environment for cybercriminals to commit crimes in cyberspace. Unlike the surface web, which is indexed by search engines and often linked to identifiable users and host providers, the dark web operates through anonymity-enhancing technologies such as the tor browser.

These technologies conceal users' identification, such as the IP addresses and their physical locations, making it difficult for law enforcement to trace criminals and track activities online. While the feature of anonymity on the dark web also protects and serves legitimate purposes, this includes protecting journalists, activists, and whistleblowers, often working in oppressive work environments.

Thus, serving the dual purpose of anonymity and anonymous based technology that facilitates cybercrime. Despite its reputation and holdings, the dark web represents only a fraction of the internet, while the surface web and deep web account to vast majority of the internet.

History of Dark Web

Dark Web is a non-indexed part of the internet which is used by those who are trying to control access to personal information and prefer great desire for secrecy. This motivates them to commit illegal crimes on the internet. Hiding the identities of those involved in cybercrimes along with crypto exchanges on the dark web is inherent to cybercriminals. Dark web transactions often represent a range of international crimes, tax evasion, and failure to follow rule of law. The internet is divided into three distinct layers; Surface Web, Deep Web, and Dark Web. These represent distinct parts of the online world with varied purposes, accessibility features, and levels of security. Understanding these layers is essential, as each plays a unique role in the digital ecosystem.

Surface Web³, also known as the Indexed Web, is a portion of the internet that is publicly accessible and is indexed by popular search engines. It represents websites that users can easily access through standard web browsers and that do not require authentication. The Deep Web⁴ refers to the internet that is not indexed by traditional search engines. Contrary to popular belief, the deep web is not illegal; rather, it makes approximately 90–95% of the internet's volume. Content in the deep web requires authentication, passwords, and permissions before access is granted. The dark web is a subset of the deep web that is intentionally hidden which requires tor browser to gain access. Unlike surface web, websites on dark web cannot be accessed using standard web browsers. It uses advanced encrypted technology that conceals identities and user locations using layered encryption, a process known as onion routing.

Table 1: Chronology of the Dark Web

Timeline	Chronology of Events	Significance
1966	Development of ARPANET	Foundation of Internet
1983	Internet adopts TCP/IP	Standardization of Internet Protocols
1990	World Wide Web	Surface Web Established
1993	US Navy Initials Onion Routing Research	Conceptualization of Anonymous Internet
1995	Onion Project	Research Aimed to Protect Information
1997	Onion Routing Prototype	Demonstrated Anonymous Routing over the Internet
2002	TOR Released	TOR enables Anonymous Browsing
2004	TOR is Open Source	Researchers Contribute to Improving Anonymity
2011	Silk Road Initiated	Dark Web Marketplace Released
2012	Expansion of Dark Web	Sale of Stolen Data, Hacking, Malware
2015	Ransomware-as-a-Service	Ransomware Toolkit Available
2016	Cybercrime-as-a-Service	Malware, Phishing, Botnets
2018	Criminal use of Cryptocurrency	Use Cryptocurrency to Obscure Financial Transactions
2020	COVID-19	Sale of Fake COVID Vaccines and Disinformation
2025	Generative AI-Enabled Cybercrimes	AI-Enabled Phishing, Deepfakes, Malware

Source: Compiled and Created by Author

Table 2: Comparison Between the Deep and Dark Web

Stricture	Deep Web	Dark Web
Definition	Un-Indexed by Search Engine	Subset of Deep Web
Relation	Encompasses all web content that is not searchable	Exists within Deep Web
Accessibility	Accessible using Standard Web	Accessible using Tor Browser
Purpose/ Aim	To Protect Information	To Provide Anonymity
Visibility	Visible to Select Users	Hidden from Surface Web
Users	Researchers, Businesses, Banks, Governments and Organizations	Journalists, Whistleblowers, Intelligence, Cybercriminals
Access	Chrome, Firefox, Safari	Tor Browser
Anonymity	Moderate	High
Status	Legal	Subject to Jurisdictions
Hosting	Standard Web Servers	Hidden Web Servers
Risk Level	Low	High
Malware Risk	Low	High
Fraud Risk	Low	High
Internet Volume	Estimated 90% of the Internet	Estimated 1% of the Internet

Source: Compiled and Created by Author

Dark Web and Cybercrimes

Dark Web today has become a safe haven for those individuals and cybercriminals who seek to maintain anonymity by concealing their identity online and dodge law enforcement. It is a hazardous place where cybercriminals operate with full anonymity. Cybercrime refers to criminal activities carried out using computers, digital devices, and internet. The dark web facilitates various cybercrimes by providing marketplaces, communication channels, and financial systems that are difficult to detect for law enforcement. Here are some of the cyber-enabled crimes on the dark web.

- **Stolen Goods**

Dark Web hosts a variety of illicit marketplaces⁵. Cybercriminals sell stolen goods and information on these marketplaces. These markets function as underground economies, allowing cybercriminals to buy and sell illegal goods and information while attempting to conceal their identities. Stolen goods received through; physical robbery, stolen antiques, organized crime, online scams, cyber theft, digital fraud, hacking, are sold on these marketplaces online. This includes; consumer electronics (smartphones, laptops, tablets, electronic gadgets), luxury goods (watches, jewelry, antiques, designer handbags), counterfeit items (fake pharmaceuticals), digital assets (software licenses, hacked crypto wallets) and corporate information (business documents, intellectual property theft, trade secrets)

- **Data Dump**

Data Dump⁶ is an extensive collection of stolen information (data) procured through cyberattacks, which include; phishing, malware, insider theft, data breaches, and data procured through digital hacking. The term data dump refers to the bulk release of information on the internet. Data dump may contain personal information including; individual names, home addresses, phone numbers, email addresses, dates of birth, password and login credentials. Financial information, including; payment of debit/credit card, bank account details, medical records, insurance records, and government source documents, can go public through such data dumps. Similarly, corporate employee databases and consumer databases, confidential business documents and internal communications may be leaked online for political and economic reasons.

- **Exploit Markets**

Exploit Markets are those where software vulnerabilities are sold on the dark web even before security patches are released. Zero-Day⁷ exploits cyber vulnerabilities, where the vendor has yet to release security update. Exploit markets serve as a gray marketplace for buying and selling zero-day exploits. These underground marketplaces provide opportunities for cybercriminals to trade such cyber vulnerabilities, including; malware, hacking, ransomware, spyware, remote access trojans, stolen credentials, and cyber tutorials. Such marketplaces operate using cryptocurrencies, making anonymous crypto payments, and act as a major hub for cybercrime-as-a-service.

- **Drugs Trafficking**

Owing to the anonymous⁸ nature of the dark web and its significant advantages, one can create an anonymous profile online without being noticed by law enforcement. This advantage gives a huge impetus to the drug cartels and their consumers to sell banned contraband items. The feature of anonymity protects both; the buyer and seller, where both meet for trade without the fear of losing identity. Such discreet online behaviors have significantly increased the comfort levels of drug cartels and have provided confidence in reaching wider markets, predominately the youth. International drug cartels transcend geographical boundaries that often go beyond the reach of law.

- **Terrorism**

Dark Web and Terrorism⁹ seem to complement each other, as the latter requires an anonymous network for communication, command, and control. It would be difficult for such individuals to upkeep their operations on cyber space with ease, as their sites and servers could be potentially targeted by law enforcement. In a yet another significant challenge to the state, the use of the internet for terror purposes could cause significant challenges, including; loss of life, damage to critical infrastructure, misinformation and disinformation which pose serious risk to cyberspace, cybersecurity, and national security. Terrorism is often used as a tool to achieve social, political, and ideological objectives through the use of criminal intimidation, coercion, and extreme violence. Today, online terror threats extend to the banking sector, defence sector, military installations, healthcare systems, power grids, air traffic control, water control systems, and internet of things. Websites such as Silk Road¹⁰ act as anonymous marketplaces for selling

illegal goods and banned substances. These sites appear unlike any other commercial website, which host illegal goods and services on dark web.

- **Hacking**

Hacking refers to gaining illegal access to computer systems and its network in order to exploit its weaknesses. It is an illegal activity wherein hackers seek to compromise digital devices and information networks, which include; computers, computer systems, computer networks, mobile devices, internet of things, websites and its servers. It is a process where hackers try to intrude into the network in an unauthorized manner, without the knowledge of the rightful owner. It is a technical terminology that requires sound technical capabilities. One cannot perform the art of hacking without prior knowledge of computers. It requires capabilities in computer programming along with the ability to exploit computer weaknesses and erase digital footprints.

- **Malware Distribution**

Malware is a malicious program that automates computers to spread further into other computer networks and their systems using the internet. It can perform complex tasks remotely and execute cyber operations until aim is achieved. Users who visit suspicious website, open rogue cyber links, or visit unverified URL's can potentially download and install malware on their computers. Malware further creates botnets, which can be remotely accessed to perform denial of service attack.

Impact of the Dark Web and Cybercrime

- **Disruption of Critical Infrastructure**

Critical Infrastructure¹¹ includes; banks, power grids, transport, chemical, nuclear, healthcare, and defence industries. Any disruption in the sector poses serious risks to public safety and national security. Disruptions to critical infrastructure can lead to widespread chaos, economic losses, harm to human lives, and damage to reputation. Critical infrastructure acts as a core component of national development and national security. Its protection is essential as it gives smooth access to human life. Any disruption in these sectors would result in chaos that could bear enormous financial costs for damages and repairs. With the infusion of technology into critical infrastructure, these systems have become vulnerable to cyber-attacks.

- **Psychological and Social Impact**

Victims of cybercrime often experience psychological experiences that include; anxiety¹², despair, trauma, helplessness due to the violation of privacy and loss of control over personal information. Cybercrime carries long-lasting psychological effects, thereby eroding trust in digital technologies and reducing faith in public institutions. Since information is private, if compromised, the information could go public. This includes; credit/debit card numbers, chat histories, browsing habits, online purchase history, and social security numbers. A single cyber intrusion is enough to cause significant damage to data companies and their reputation, as companies that hold large amounts of information are vulnerable to cyber-attacks. Dark web enables cybercrimes to carry broad range of societal implications. This includes; loss of confidence, panic, chaos, erosion of trust, question morality and cyber ethics. Similarly, proliferation of cyber technologies to commit large-scale cybercrimes aggravates social inequalities, as marginalized communities carry the risk of cyber exploitation.

- **Financial Losses**

Though dark web is not linked to financial losses, it provides an ecosystem for stolen data and illicit services, enabling a wide range of cybercrimes. Such illegal activities can cause financial losses to individuals, businesses and organizations through financial fraud, ransomware, identity theft, intellectual property theft, and business disruption. Effective security measures against financial losses include; public awareness, software updates, incident response, and disaster management plan. Cybercrimes can cause significant losses to businesses, governments, and organizations worth billions of dollars.

Dark Web Motivations

- **Ideological Systems**

Cybercriminals are often driven by ideological motives, that use cyberspace as a medium to advance political, social, economic, or religious objectives. These actors may engage in cyberterrorism, hacktivism, and propaganda to achieve their desired objective. Ideologically motivated cybercriminals carry far-reaching consequences with their active contribution towards criminality, social unrest, polarization, and escalating regional tensions. With dark web providing channels of encrypted

communications towards people with different sets of political, social, and religious beliefs. This could be potentially misused by rogue individuals in order to promote extremism, coordinate unlawful activities online, and distribute prohibited content.

- **Vendetta**

At times, many cybercriminals invoke personal vendettas¹³ and grudge against business, government and organizations through cyberstalking, online harassment, defamation, intimidation, extortion, hacking and revenge. Personal vendettas can easily escalate into cybercrimes, posing serious risks to cyberspace, individuals' safety, and mental well-being. Using dark web to facilitate personal vendetta can cause serious crimes, resulting in criminal trial, law enforcement, forensic investigations, prosecution, and imprisonment.

- **International Tensions**

International tensions have now extended into cyberspace, wherein dark web has become an extended environment for nation states, non-state actors, cybercriminals, hacktivists, and extremist groups to communicate, exchange, and coordinate information. Although much cyber conflict occurs on surface web or deep web networks rather than on the dark web it facilitates certain activities using anonymity feature and its hidden services. State-sponsored espionage¹⁴ represents a significant risk in this direction, as nation-states and intel agencies leverage dark web to gather intelligence, conduct covert operations, share information, undermine, and destabilize adversarial cyber networks. Covert actions may include; targeting government institutions, military installation, critical infrastructure, and sabotaging¹⁵ strategic assets online.

Conclusion

Thus, dark web represents a complex and dynamic segment of the internet, which was originally designed to protect privacy and enhance anonymity and has now become a hotbed for cybercriminals that enable illegal marketplaces, data breaches, trafficking, terrorism, hacking, and malware distribution. Today, dark web supports organized cybercrime by providing access to stolen goods, exploit markets, and ransomware-as-a-service. Critical infrastructure also remains at heightened risk while individuals and organizations suffer from psychological and financial harm, resulting in damage and erosion of trust. The impact of cybercrimes originating from dark web is profound and complex, which underlines the need for a collaborative approach and robust response. This requires immediate attention from governments, law enforcement, cybersecurity professionals, and netizens in order to safeguard the integrity of cyberspace and protect information.

References

1. <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web>
2. <https://www.kaspersky.com/resource-center/threats/spyware>
3. <https://www.britannica.com/technology/surface-web>
4. <https://www.group-ib.com/resources/knowledge-hub/deep-web>
5. <https://nordstellar.com/blog/top-10-dark-web-marketplaces>
6. <https://help.cdmplus.com/administra1/data-dump>
7. <https://security.stackexchange.com/questions/33314/what-is-zero-day>
8. <https://www.merriam-webster.com/dictionary/anonymous>
9. <https://www.interpol.int/en/Crimes/Terrorism>
10. <https://www.avast.com/c-silk-road-dark-web-market>
11. <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience>
12. <https://www.unicef.org/parenting/mental-health/what-is-anxiety>
13. <https://dictionary.reverso.net/english-definition/vendetta>
14. <https://www.geeksforgEEKS.org/ethical-hacking/what-is-cyber-espionage>
15. <https://lieber.westpoint.edu/intelligence-wars-sabotage-shadows-conflict>

