e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:07/July-2024 Impact Factor- 7.868 www.irjmets.com

THE RISING IMPACT OF THE DARK WEB ON CRIMINAL ACTIVITIES

Sagar Y*1

*1Department Of MCA, Brindavan College Of Engineering, Bengaluru, Karnataka, India.

ABSTRACT

Cyber thieves, terrorists, and state-sponsored spies use the Dark Web due to its difficulty to trace and its anonymity. Cybercrime on the Dark Web mirrors real-world criminality but thrives due to the platform's unpredictable environment. Evaluating Dark Web crime threats is essential for discovering remedies to cybercrime. This study examines Dark Web crimes, their consequences, enforcement tactics, and future measures to reduce threats. Using a Systematic Literature Review (SLR) method, we analysed 65 relevant articles to provide guidance on rising Dark Web criminal dangers. Our findings offer a comprehensive understanding of Dark Web crimes, assess their social, economic, and ethical impacts, and analyse challenges and techniques for locating criminals. We highlight the need for more research to identify criminals, emphasize the importance of forensic analysis of crypto markets and forums, and suggest that Dark Web anonymity can aid in catching criminals. Properly analysing digital evidence is crucial for law enforcement to seize criminals and shut down illicit activities.

Keywords: Dark Web, Cybercrime, Forensic Analysis, Law Enforcement, Cyber Security, Terrorism.

I. INTRODUCTION

The World Wide Web (WWWW) is a complicated system that contains an enormous amount of digital data. Standard search engines such as Google and Yahoo provide access to the everyday Internet. However, huge portions of the Internet are unindexed and unavailable to traditional search engines. The Deep Web, which makes up around 96 percent of the WWW, is a hidden component of the Internet. The Dark Web, often knownas the Dark Net, is a subsection of the Deep Web that is mostly utilised for illegal purposes.The Dark Web is used by 57 percent of people for criminal activity and illicit content. Illegal substances, weapons trafficking, child pornography, stolen financial information, and illegal talks are just a few examples.

When the US Federal Bureau of Investigation (FBI) shut down the most well-known DarkWeb marketplace Silk Road in 2013, the public became aware of these criminal operations. The Dark Web's hidden wiki and deep search engines are the best places to look for malevolent intents and criminal information. These sites provide access to a large number of other Deep Web links. The anonymity provided by Dark Web services is one of the keychallenges forensic analysts face when investigating illegal behaviour on the Dark Web. Anonymous services like Tor, Freenet, I2P, and JonDonym frequently utilize the Dark Web's contents and services.

The TOR network, which allows users to surreptitiously transfer information anonymously via peer-to-peer connections rather than a centralised computer server, is the most popular service on the Dark Web. The U.S. Naval Research Laboratory created this service in 2002with the goal of accessing banned content, circumventing censorship, and maintaining the secrecy of critical communications. Due to the TOR network's anonymous architectural structure, monitoring the Dark Web is extremely difficult. Because of its untraceable and difficult to take down architecture, criminals use the Onion Router (TOR) to navigate the Dark Web. One of the reasons for the enormous demand on security services and law enforcement to monitor and trace activities on the Dark Web is because of this.

Criminals typically use the TOR to set up a relay station and hide their nefarious activity on the Dark Web. As a result, when law enforcement uses the TOR browser to trace the IP address to the identity of the perpetrated crime, they only find the latest TOR exit relay. Various tactics and methods have been created by researchers to monitor and detect variouscrimes and criminals on the Deep Web. The US Defense Advanced Research Projects Agency (DARPA) designed and implemented the Memex Project, which is one of the mostsuccessful data mining tools on the Dark Web. In a study, mapping the hidden services directory, social site monitoring, customer data monitoring, semantic analysis, and marketplace profiling were discussed as approaches to pro-actively monitor the hidden areas of the Internet. Law enforcement has used a variety of measures to track down criminals, including social media, IP addresses, user monitoring, and Bitcoin account monitoring.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:07/July-2024 Impact Factor- 7.868 www.irjmets.com

II. LITERATURE REVIEW

Table 1. Literature Review

SL NO	TITLE	AUTHORS	IEEE TRANSACTION /JOURNAL&YEAR	METHODOLOGY
1	FbHash: A New Similarity Hashing Scheme for Digital Forensics	Somitra Kumar Sanadhya, Monika Singh	2019	A new Approximate Matching scheme termed as - FbHash. We show that our scheme is secure against active attacks and detects similaritywith 98% accuracy.
2	Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time	Meropi Tzanetakis	2018	A systematic measurement analysis of structures and trends on the most popular anonymous drug marketplace, and discuss the role of cryptomarkets in drug distribution.
3	Analysis of fingerprinting techniques for tor hidden services	Andriy Panchenko, Asya Mitseva	2017	A novel two-phase approach for finger printing hidden services that does not rely on malicious Tor nodes. In our attack, the adversary merely needs to be on the linkbetween the client and the first anonymizationnode
4	Sockpuppet gang detection on social media sites	Quanyuan WU, Weihong HAN	2016	multiple community detection algorithms todetect SPGs in the network. User accountsin the same SPG are considered to be controlled by the same individual or organization.
5	Detection of severeSSH attacks using honeypot servers and machine learning techniques	Gokul Kannan Sadasivam, Chittaranjan Hota	2017	The machine learning techniques with appropriate parametersand feature selection technique. A real-timedetection model that is tested on a public server also.

III. METHODOLOGY

This section describes the Systematic Literature Review (SLR) method used for conductingthis review. We have also considered some recent studies with SLR method to apply in our work. SLR uses systematic methods to define research question, conduct literature search, screen the findings, extract the data from the selected findings, analyze and synthesize the findings qualitatively or quantitatively. The methodology includes defining (i) the research questions (ii) relevant data sources and the search procedures (iii) inclusion and exclusion criteria (iv) extraction of data (v) analysis and synthesis of the data

RESEARCH QUESTIONS

Providing the summary of emerging crimes happening in the Dark Web with their consequences and defense techniques is the main goal of this work. Thus, the following research questions and the motivations are as follows:

- RQ1: What are the rising threats in the Dark Web crimes?

Identifying the type of Dark Web threats globally can help to show how the illegal contents and the services are

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:07/July-2024 Impact Factor- 7.868 www.irjmets.com

accessed and what their consequences are. This raises the challenges and importance of creating better technologies and law enforcementto trace the criminals.

- RQ2: What types of techniques are applied to locate the criminals in Dark Web?

Identify the law enforcement methods, applied and available technologies for tracing and detecting the crimes and criminals in the Dark Web. It gives the future path to apply different strategies with latest technologies along with law enforcement to defeat the cyber-criminals plan.

SEARCH STRATEGY AND SELECTION

We have followed the search strategy guidelines stated, which is explained below in details. To collect the data for the review papers, electronically-based search was performed from IEEE Xplore, ScienceDirect, Springer, Scopus, ACM Digital Library and Google Scholar.

We included in our search term the Dark Web crimes mentioned in and. We have used the terms from our research questions. Boolean search operation with ANDS and ORs has been implemented to specific phrases. The search terms used for retrieving our relevant articles are presented in Table 1. However, this is to mention that different search terms have been used for retrieving relevant publications. Also, a search for additional articles from the references of the relevant articles found was considered. The matching of the strings in the search terms from the digital libraries are based on the title, abstract and keywords of the papers except the Springer library which does not allow to restrict the search in specific parts of the paper. We did the filtering and screening for selecting the most relevant papers based on the inclusion and exclusion criteria discussed below. The inclusion and exclusion criteria followed in this survey are described in Table 2 and 3 respectively. After applying these screening steps with the inclusion and exclusion criteria 65 articles were selected for this review paper. The selected publications are listed in Appendix (A). After applying the inclusive and exclusive criteriain our filtering process we ended up with 65 papers. The overall SLR article selection procedure applied in our survey paper is described in the Figure 1. Some of the selection techniques are described as follows.

- Automatic search: Using the search terms on the six database libraries mentioned with automatic search we couldcollect 1920 papers.
- Title-based selection: For a fast article picking method title based selection was performed. We choose the articles from the title of the paper that are relevant to our SLR. This made the number of papers to 581.
- Duplication removal: In this case duplicate papers were removed as some of the database indexes papers are available in the other databases. After removing the duplicates, the number of articles reduced to 393.
- Abstract-based selection: To check whether the selected 372 papers are related to our SLR, the abstract of the papers were read. The irrelevant abstract articles were disregarded at this stage and 100 papers were selected.
- Full-text selection: Each of the 100 papers was completely read through and 65 papers were selected based on this.

Out of 65 papers, 18 were selected from IEEE Xplore, 22 papers were from Google Scholar, 6 articles were chosen from ScienceDirect, 9 papers were selected from Springer, 5 papers were selected from Scopus and the rest 5 papers were extracted from ACM Digital Library.

Table 2. Search term for selection of literatures

SI	Search Term
1	"Dark Web" AND " crimes" OR "Dark Net" AND "cyber security"
2	"Dark Web" AND "threats" OR "attack" AND "crime rates"
3	"crypto markets" OR "Dark Net marketplaces" OR "bit coin" OR "silk road" OR "TOR"
4	"illicit" OR " illicit Products" AND "Dark Net"
5	"techniques" AND "Dark Web" OR "strategies" AND "Dark Web"
6	"law enforcement" OR "darpa" OR "memex" AND "challenges" AND

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:07/July-2024 Impact Factor- 7.868 www.irjmets.com

	"Dark Web"
7	"drugs" OR "human trafficking" OR "fraud" OR "prostitution" OR "terrorism" Or "data breach" AND "Dark Web"

Table 3. Exclusion criteria for selection of literatures

EC#	Description
EC1	Exclude the duplicate articles obtained by authors and/or different libraries
EC2	Exclude articles those specifies Dark Web but do not include crime threats or crime locating techniques
EC3	Exclude cyber security defense articles not related to Dark Web

Table 4. Inclusion criteria for selection of literatures

IC#	Description
IC1	A study that is focused on Dark Web related crimes and demonstrates the crimes, consequences and assess techniques
IC2	A study that is based on the tracing techniques and technologies for locating the criminals in the Dark Web for cyber security
IC3	The search term keywords in Table.1 applies the operators of search syntax OR, AND. AND operator signifies that both keywords must be present in the search queries and OR means that at least one keyword must be present in the queries searched
IC4	Studies published in English language
IC5	Include data from journals, conferences and web articles published between the year 2003 to 2019
IC6	Include abstract based and full-text studies

DATA EXTRACTION AND SYNTHESIS

To answer our research questions in this systematic literature review the procedure of data extraction and analysis of the data extracted from the filtered papers is discussed in this section. The extraction of data from the filtered articles has been done based on the data extraction form. Microsoft Excel spread sheet was used to record the extracted data.

To evaluate article suitability in accordance to answer the research question the quality attribute rules were applied. 6 QARs were identified and each one is worth 1 mark out of 10. The score is as follows ‘‘fully answered’’=1, ‘‘above average’’=0.75,’’ average’’=.50 and ‘‘below average’’=0.25,’’not answered’’=0. The overall score of the article will be the summation of marks obtained from the 6 QARs. If the result was 3 or higher, the article was considered to answer our RQs otherwise was excluded. The QARs are shown in Table 5. For data synthesis on the extracted data, we have used different procedures that aggregate the evidence to answer our RQs. The demographic data of the reviewed articles have been analyzed using descriptive statistics.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:07/July-2024 Impact Factor- 7.868 www.irjmets.com

Table 5. The QARS of this SLR

QAR#	Description
QAR1	Are the objectives of the research articles clearly defined?
QAR2	Are the Dark Web crime backgrounds addresses properly?
QAR3	Are the Dark Web crimes tracing techniques used clearly defined?
QAR4	Are the articles comprehensive and take into consideration past and current literature?
QAR5	Are the methods used to analyze the results appropriately?
QAR6	Do the articles identify the gap of knowledge?

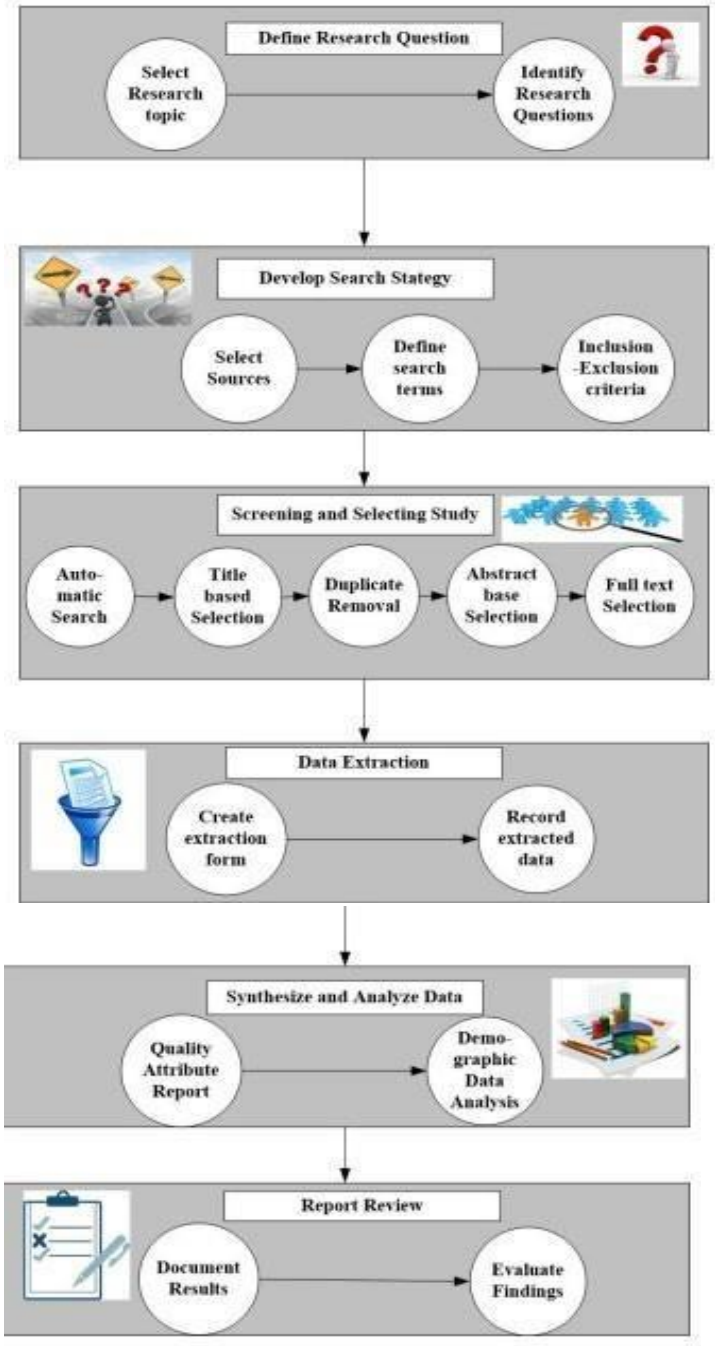

Figure 1. Applied SLR Methodology

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:07/July-2024 Impact Factor- 7.868 www.irjmets.com

IV. RESULT AND DISCUSSION

In this section, we'll respond to the two research questions and discuss the findings of this systematic literature review. The first research question (RQ1) aims to identify the growing concerns in Dark Web criminal activity. This will be addressed in subsection A. With subsections III.A.1 through III.A.8, this subsection responds to our RQ1 by providing an overview of the hazards in the Dark Web resulting from illegal activity. Our second research question (RQ2) examines the various approaches used to track down offenders on the Dark Web In subsection B, we explained how to respond to and analyze this. The analysis of the strategies and procedures used to combat these risks is addressed in sections III.B.1.a to III.B.2.i of our RQ2. Following that, we give the third paragraph III.C, which summarily evaluates the substance of the 65 retrieved studies and their contributions.

CRIMINAL ACTIVITY THREATS IN THE DARK WEB(RQ1)

We identified eight key crime dangers on the Dark Web based on the articles we chose, which answers our RQ1. The following is a list of crime threats:

- Human trafficking and sex trafficking
- Pornography industry
- Assassinations and its marketing
- Drug transactions
- Child Pornography
- Terrorist
- Markets for Cybercrime Tools and Stolen Data
- Dark Net currency exchange using bitcoin

TECHNIQUES TO LOCATE CRIMINALS IN DARK WEB(RQ2)

Cybercrime on the Dark Web is identical to crime in the real world, with the exception that law enforcement finds it difficult to follow virtual crime on the Dark Web. One of the biggest issues that certain forensic analysts may confront when trying to examine criminal activities is the anonymity afforded by Dark Web services. As a result, forensic investigation of illegal behavior is hampered. On the Dark Web, many crime detection investigations have been conducted in order to find crimes or offenders. In the subsections under law enforcement and detection methods, we'll see how detection techniques and law enforcement methods are used and begun for this aim. This section answers our RQ2

- **Law Enforcements**

Because cybercriminals' abilities have grown, smaller law enforcement agencies lack the technical expertise to combat specific offences. Criminal law, civil law, and regulatory law are all forms of laws that apply to criminal behavior on the Dark Web.Criminal law is concerned with crimes committed at the municipal, state, and federal levels of government. The punishment may be anything from a fine to life in jail. Depending on the state where the crime took place, the penalty might be death. Civil law refers to a person or organization who has been found guilty and has been ordered to pay a fine or perform community service as part of their punishment. In regulatory law, a jurisdiction's regulatory agency has the authority to levy penalties as a form of punishment for certain activities. Regulatory authorities have the authority to stop persons or businesses from doing business if they are not in compliance.

- **Social Media**

Social networking and the Deep Web can be used together to detect illicit activity on the Dark Web. Suspects are identified through various media such as Twitter, YouTube,and Facebook. Cybercriminals use social media sites like Facebook, Snapchat, Instagram, WhatsApp, Telegram, and other social media platforms to communicate and sell stolen identities, credit card numbers, and other information, according to RSA.

The use of these platforms by cyber criminals is due to the ease with which they may share and spread anything, including malware, on social media sites. When compared to other websites, these platforms have more tricks up their sleeves, such as advertisements, sharing buttons, and plug-ins. Furthermore, the fact that hundreds to

thousands of users are connected on these platforms makesit easier for thieves to transmit malware to a bigger audience. Last year, a six-month global study on social media cybercrime by criminology experts at the University of Surrey in the United Kingdom revealed annual earnings of cybercriminals exploiting prominent social platforms to be approximately $3.25billion.

On the plus side, social networking is creating avenues for law enforcement agents to solve crimes. Because social platforms have a huge number of users, tips can be acquired through their online presences as well as observation of crimes committed in their communities. The arrest of Raderius Glenn Collins, a Florida thief who made a seven-minute Facebook video gloating about a $500,000 jewellery heist that received 3,000 views; Derek Medina, 33, was sentenced to life in prison for the second-degree murder of his wife. Maxwell Marion Morton was charged with first-degree murder after he posted a selfie ofa student who had been shot in the face over SnapChat; 71 people were arrested by Cincinnati police following a 9-month investigation using social media to identify key gang members.

The University of Cincinnati's Institute of Crime Science merged information acquired on social media with police records and reports to create a link between suspects, which assisted the police in apprehending the gang. According to LexisNexis, more than 80% of police agencies use social media as an investigation tool. LexisNexis describes the use of social media ininvestigations between 2012 and 2014.

- **Crime Detection**

The relevance of finding the perpetrators and the connected crimes is incalculable in combating the developing crimes that are growing in the anonymous Dark Web. Although analyzing the untraceable anonymous networks used by cyber criminals is a difficult endeavor, numerous approaches and procedures have been created that can be employed in this area.

Hash Value Analysis

Sock Puppets and Informant Analysis

Network Analysis Methodologies

V. CONCLUSION

In particular, this SLR includes a detailed overview of Dark Web crime threats, technological and forensic issues associated with anonymous network architecture, and detection methods, algorithms, tools, and strategies used to track down crimes and offenders on the Dark Web. Cyber thieves are growing increasingly savvy in their approachto evading detection on the Dark Web. As a result, the stakes have been raised. International boarder is one of the most difficult tasks for law enforcement and security services. The sheer magnitude of the dark web needs more effective techniques to reducing the Dark Web's potential hazards. Advanced methods must be used to track down the black market and the transactions that take place there in order to catch the offenders. The Dark Web's unindexed, fractured, and multilayer structure makes it more difficult to discover crimes. Because the Dark Web environment is inherently unpredictable, with old sites disappearing every day and new sites appearing, forensic law authorities must acquire sufficient digital evidence to ensure that they can overcome barriers in capturing and punishing perpetrators.

VI. REFERENCES

[1] K. V. Açar, ‘‘Webcam child prostitution: An exploration of current and futuristic methods of detection,’’ Int. J. Cyber Criminol., vol. 11, no. 1, pp. 98–109, 2017.

[2] A. Afilipoaie and P. Shortis, ‘‘From dealer to doorstep-How drugs are sold on the dark net,’’ GDPO Situation Anal., Swansea Univ., Global Drugs Policy Observatory, Swansea,U.K., Tech. Rep., 2015

[3] I. Agrafiotis, A. Erola, M. Goldsmith, and S. Creese, ‘‘A tripwire grammar for insider threat detection,’’ presented at the Int. Workshop Manag. Insider Secur. Threats(MIST), 2016.

[4] M. Ahmed, A. N. Mahmood, and M. R. Islam, ‘‘A survey of anomaly detection techniques in financial domain,’’ Future Gener. Comput. Syst., vol. 55, pp. 278–288, Feb. 2016

[5] J. Aldridge and D. Décary-Hétu, ‘‘Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets,’’ Int. J. Drug Policy, vol. 35, pp. 7–15, Sep. 2016

[6] A. Bancroft and P. Scott Reid, ‘‘Challenging the techno-politics of anonymity: The case of cryptomarket

users,'' Inf., Commun. Soc., vol. 20, no. 4, pp. 497–512, Apr. 2017.

[7] A. Baravalle, M. S. Lopez, and S. W. Lee, ''Mining the dark Web: Drugs and fake IDS,'' presented at the IEEE 16th Int. Conf. Data Mining Workshops (ICDMW), Dec. 2016.

[8] M. J. Barratt, J. A. Ferris, and A. R. Winstock, ''Safer scoring? Cryptomarkets, social supply and drug market violence,'' Int. J. Drug Policy, vol. 35, pp. 24–31, Sep. 2016

[9] H. Bleau. (Apr. 24, 2019). Social Media and the Digital Transformation of Cybercrime. RSA Security. [Online]. Available:
https://www.rsa.com/enus/blog/2019-04/social- media-and-the-digital-transformation-of cybercrime

[10] S. Brown (Apr. 30, 2019). Cybercriminals ramping up fraud attacks on social media, says report. Cnet. [Online]. Available:
https://www.cnet.com/news/cybercriminals-are-ramping-up-fraudattacks-on-social-media-says-report/