big data and cognitive computing

MDPI

Review

Weaponization of the Growing Cybercrimes inside the Dark Net: The Question of Detection and Application

Amr Adel [1,2,3,*] and Mohammad Norouzifard [4,5]

[1] School of Computing, Eastern Institute of Technology, Auckland 1010, New Zealand
[2] School of Information Technology, Torrens University Australia, Adelaide, SA 5000, Australia
[3] School of Information Technology, International College of Management Sydney, Manly, NSW 2095, Australia
[4] School of Tech, New Zealand Skills and Education College, Auckland 1010, New Zealand; mohammad@nzse.ac.nz
[5] Auckland Bioengineering Institute, University of Auckland, Auckland 1010, New Zealand
* Correspondence: avandenadel@eit.ac.nz or amr.adel@torrens.edu.au or aadel@icms.ed.au

Abstract: The Dark Web is a subset of the Deep Web, requiring special browsers, the Dark Net refers to encrypted networks, the Deep Web encompasses non-indexed online content, and darknet includes unused IP address networks. The Dark Net has become a hotbed of cybercrime, with individuals and groups using the anonymity and encryption provided by the network to carry out a range of criminal activities. One of the most concerning trends in recent years has been the weaponization of cybercrimes, as criminals use their technical skills to create tools and techniques that can be used to launch attacks against individuals, businesses, and governments. This paper examines the weaponization of cybercrimes on the Dark Net, focusing on the question of detection and application. This paper uses a Systematic Literature Review (SLR) method to appraise the Dark Web, examine the crimes and their consequences and identify future measures to reduce crime threats. Data from 88 relevant articles from 2011 to 2023 were extracted and synthesized, along with the latest data from 2024 to answer research questions, providing comprehensive knowledge on growing crimes; assessing social, economic, and ethical impacts; and analyzing established techniques and methods to locate and apprehend criminals.

Keywords: dark web; dark net; weapon; TOR; cybercrimes; government

Citation: Adel, A.; Norouzifard, M. Weaponization of the Growing Cybercrimes inside the Dark Net: The Question of Detection and Application. *Big Data Cogn. Comput.* **2024**, *8*, 91. https://doi.org/10.3390/bdcc8080091

Academic Editor: Fabrizio Baiardi

Received: 22 May 2024
Revised: 23 July 2024
Accepted: 1 August 2024
Published: 14 August 2024

1. Introduction

The World Wide Web (WWW) is a sophisticated network that contains an enormous amount of digital data. The regular Internet that people use daily is accessible through search engines like Google and Yahoo. However, there is a significant portion of the Internet that is not indexed and cannot be found through regular search engines [1]. This hidden portion of the Internet is known as the Deep Web and is estimated to constitute approximately 96% of the WWW [2]. Within the Deep Web, there is a subset mostly used for illicit purposes called the Dark Web or Dark Net [3]. Criminal activities and illegal content are prevalent in this area. The Dark Web is known for hosting various illegal activities, such as drug dealing, weapons trafficking, child pornography, financial fraud, terrorist communication, and more [4]. When the US Federal Bureau of Investigation (FBI) closed the infamous Silk Road marketplace operating on the Dark Web in 2013, it brought public attention to these criminal activities [5]. Hidden wikis and deep search engines are used to access illicit content on the Dark Web, providing access to numerous links in the Deep Web [6]. One significant challenge forensic analyst face when investigating criminal activities on the Dark Web is the anonymity provided by Dark Web services.

The Dark Web provides various services and content that can be accessed without revealing one's identity, using platforms like Tor, Freenet, I2P, and JonDonym [7]. Among these, the TOR network is the most widely used, enabling anonymous information sharing

via peer-to-peer connections instead of relying on a central server. Originally developed by the U.S. Naval Research Laboratory in 2002, its primary purposes were to bypass internet restrictions, evade censorship, and protect the privacy of critical communications [8]. Due to the anonymous nature of the TOR network, monitoring activities on the Dark Web is difficult, attracting criminals who exploit its secure and hard-to-disrupt framework [9]. This anonymity poses significant challenges for security agencies and law enforcement in tracking and analyzing activities on the Dark Web.

Criminals often exploit the TOR network on the Dark Web to conceal their actions. They create multiple relay points, with only the final TOR exit relay being potentially identifiable by law enforcement, which can then be used to trace back to the illicit activity. Nevertheless, researchers have devised various strategies and tools to identify and track illegal activities on the Dark Web [10]. For instance, DARPA's Memex Project has proved to be an effective data-mining tool for this purpose [11]. Other proactive monitoring approaches include analyzing hidden service directories, monitoring social networking sites, tracking customer data, conducting semantic analyses, and profiling marketplaces. Law enforcement agencies also employ various tactics, such as scrutinizing social media, IP addresses, user behavior, and Bitcoin transactions, to locate perpetrators [12].

A systematic review of the scientific literature holds significant importance in identifying research questions and justifying future research in a specific study area [13]. The aim of a Systematic Literature Review (SLR) is to identify relevant works in a particular field through a systematic study by following specific research steps and processes. Although some studies have analyzed the Dark Web, a systematic literature review on the evaluation of the Dark Web in the context of threats is still insufficiently explored, which motivated us to conduct this review. The objective of this study is to investigate emerging crime threats on the Dark Web, such as drug transactions, terrorism, human trafficking, markets for cybercrime tools, and their consequences, along with corresponding crime monitoring and locating technologies. To achieve this goal, we systematically selected and reviewed 88 articles that are relevant to our research aim. Therefore, the contributions of this paper are as follows:

In this paper, we make several significant contributions to the understanding and analysis of cybercrimes and the Dark Net:

1. Comprehensive Review: We provide an exhaustive review of the emerging criminal activities on the Dark Web, assessing their social, economic, and ethical impacts.
2. Challenges Identification: We identify and discuss the various challenges and obstacles associated with detecting and tracing criminals on the Dark Net.
3. Analytical Techniques: We evaluate established techniques and methods used by law enforcement and cybersecurity professionals to locate and apprehend perpetrators.
4. Research Insights: By addressing two primary research questions, we offer valuable insights into the nature of threats on the Dark Net and the efficacy of current countermeasures.
5. Future Recommendations: We propose future measures to mitigate crime threats, suggesting improvements in crime monitoring and locating technologies.

The first part of the paper provides an overview of the types of cybercrimes that are commonly carried out on the Dark Net, including hacking, identity theft, fraud, and the sale of illegal goods and services. The paper then explores how these cybercrimes are being weaponized by criminals to launch attacks. The second part of the paper focuses on the question of detection, examining the challenges that law enforcement agencies face in identifying and tracking criminals on the Dark Net. The paper discusses the use of technical tools such as blockchain analysis and Dark Net crawlers, as well as the importance of human intelligence and collaboration between law enforcement agencies. The final part of the paper looks at the application of cybercrime weapons, studying the impact of attacks on individuals, businesses, and governments. The paper discusses the increasing sophistication of attacks, including those carried out by state-sponsored actors, and the potential for attacks to cause significant damage to critical infrastructure. The paper also explores the

ethical and legal implications of the weaponization of cybercrimes, including the potential for unintended consequences and the need for appropriate regulations and oversight.

- This paper presents a comprehensive examination of the emerging criminal activities taking place on the Dark Web, along with the resulting impacts on social, economic, and ethical structures.
- Additionally, the study discusses the challenges and obstacles associated with identifying and tracing perpetrators of these crimes, as well as the various techniques and methods utilized to locate them and their offenses, including their limitations.

The remainder of the paper is structured as follows: Section 2 outlines the methodology employed in this research, specifically the Systematic Literature Review (SLR) technique. Section 3 presents the findings of our study. Section 4 provides detailed demographic information about the selected papers, including their distribution by publication type, year, and source. Section 5 discusses the architectures described in the selected papers, focusing on the techniques used to detect and combat Dark Net crimes. Section 6 presents the limitations and threats to validity. Section 7 identifies and discusses the various challenges associated with the ethical and social impacts of detecting and tracing criminals on the Dark Net. Section 8 discusses the future research paths that law enforcement and cybersecurity professionals should consider in order to locate and apprehend perpetrators. The last section concludes our work with a summary of the findings and directions for future research.

2. Review Methodology

This section describes the methodology employed for our analysis, specifically the Systematic Literature Review (SLR) technique. Our approach was informed by recent studies that also implemented the SLR method. The SLR approach encompasses a structured process that includes formulating research questions, performing searches for literature, screening and choosing pertinent studies, gathering data from those studies, and then conducting an analysis and synthesis of the findings, which can be either qualitative or quantitative. The steps undertaken in this review were as follows: (i) formulating research questions, (ii) pinpointing relevant data sources and search strategies, (iii) setting criteria for what to include and exclude, (iv) collecting data, and (v) analyzing and combining the collected data.

2.1. Research Questions

The primary objective of this study is to present an overview of the emerging crimes on the Dark Web, including their repercussions and methods of defense. As a result, the research questions and justifications are as follows:

Research Question 1 (RQ1): What are the emerging crime threats on the Dark Net?

Determining the kinds of hazards present on the Dark Web across the world could demonstrate how unlawful materials and services are obtained and their outcomes. This highlights the difficulties and significance of developing improved technologies and law enforcement to locate perpetrators.

Research Question 2 (RQ2): What methods are used to find the perpetrators of crimes on the Dark Net?

The goal is to identify the methods used by law enforcement and the available technologies for tracing and detecting crimes and criminals on the Dark Web. This information can help in developing future strategies using the latest technologies in collaboration with law enforcement to counteract the plans of cybercriminals.

2.2. Search Strings and Criteria

We utilized the search strategy guidelines described in [14], which are elaborated below in detail, to conduct our search. To gather data for the review papers, we conducted an electronic search on various platforms, including Google Scholar, ACM Digital Library, ScienceDirect, IEEE Xplore, Scopus, and Springer. To find relevant articles for our research,

we conducted an electronic search using various databases. Our search was guided by the search strategy guidelines described in [14]. We used terms related to Dark Web crimes mentioned in [15], as well as the research questions outlined in Section 2. We employed Boolean search operations with both "AND" and "OR" operators to find specific phrases. Figure 1 shows the search terms we used to retrieve relevant articles. However, it should be noted that different search terms may have been used to find additional publications. We also searched for additional articles by examining the references cited in the relevant articles we found.

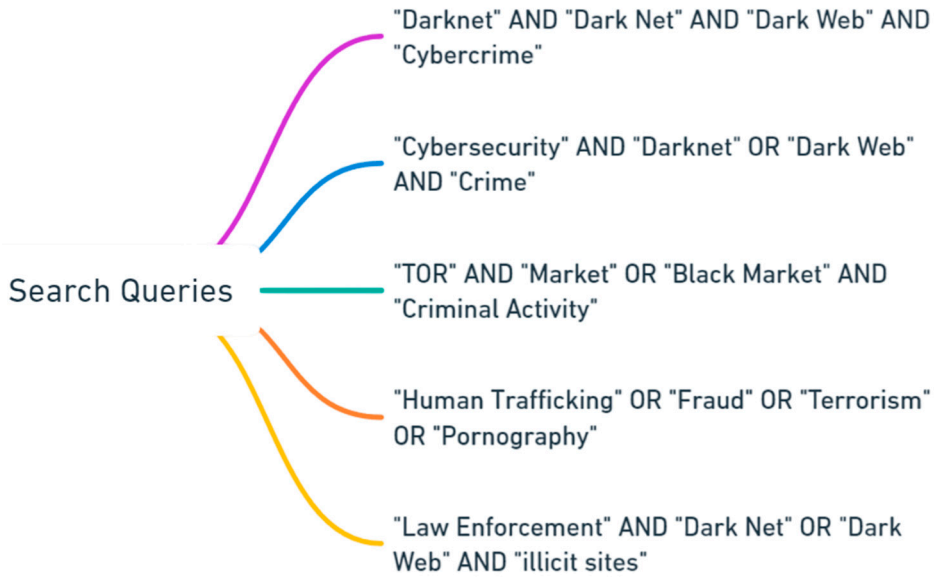

Figure 1. Search query.

To find relevant articles, the search terms were compared with the title, abstract, and keywords of the papers in digital libraries, except for the Springer library, which does not provide such restrictions. To select the most appropriate papers, a filtering and screening process was implemented based on the inclusion and exclusion criteria, which are explained in detail in Tables 1 and 2.

Table 1. Inclusion criteria.

Criterion	Inclusion Criterions
1	A study concentrates on crimes related to the Dark Web, highlighting their nature, consequences, and evaluating techniques to combat them.
2	A study is centered around tracing technologies and techniques used to locate cyber criminals operating on the Dark Web, with a focus on enhancing cyber security.
3	The search terms listed in Figure 1 use the search syntax operations of AND & OR. When using AND, both keywords must be present in the search results, whereas with OR, at least one of the keywords must be present in the search results.
4	Studies must be in English language.
5	Included studies from journals, conferences, and case studies must be from 2011 to 2023.

Table 2. Exclusion Criteria.

Criterion	Exclusion Criterions
1	Exclude articles that mention Dark Net without discussing the detection or tracing of criminals or crimes.
2	Exclude articles that do not discuss the Dark Net but are only related to cybersecurity.
3	Remove articles that have been found in more than one digital library or authored by the same author to avoid duplication of data.

Table 1 outlines the criteria for including articles in the review, while Table 2 outlines the criteria for excluding articles. We have conducted this literature search from December 2023 to February 2024. During this period, we found a total of 88 papers across various platforms. The distribution of papers from each platform is as follows: Google Scholar (25 papers), ACM Digital Library (15 papers), ScienceDirect (12 papers), IEEE Xplore (18 papers), Scopus (10 papers), and Springer (8 papers). Following these screening steps, a total of 88 articles were selected for inclusion in the review paper. After applying our filtering process based on the inclusion and exclusion criteria, we were left with a total of 88 papers for our systematic literature review. The selection procedure for these articles is illustrated in Figure 2. Some of the techniques used in the selection process are explained below:

The systematic literature review process was initiated with an extensive search across six major scientific databases—Google Scholar, ACM Digital Library, ScienceDirect, IEEE Xplore, Scopus, and Springer—using five tailored search queries to capture the broad scope of the study's theme. This initial search amassed a total of 1920 papers. Specifically, Google Scholar contributed 434 papers, ACM Digital Library 319, ScienceDirect 308, IEEE Xplore 348, Scopus 271, and Springer 240. These results highlight the effectiveness of the search queries in covering a diverse range of pertinent topics across multiple databases.

Following the initial data collection, the next phase involved a title-based screening, narrowing down the papers to 581 based on direct relevance to the review's objectives. This was followed by the elimination of duplicate papers, which reduced the number to 393. An abstract-based screening further refined this pool to 100 papers deemed highly relevant. The final step involved a thorough review of these 100 papers, culminating in the selection of 88 papers based on their significant contributions to the research topics. This structured, multi-tiered process ensured that the literature included in the systematic review was highly relevant and foundational to the overarching research goals.

During the initial literature search, papers were retrieved from various scientific databases and approximately distributed across five different search queries. This distribution aimed to evenly spread the research retrieval across all queries. For instance, from Google Scholar, which yielded a total of 434 papers, approximately 62–87 papers per query were derived, representing the upper range of the distribution. On the other hand, Springer, with a total of 240 papers, contributed about 29–48 papers per query. Other databases also contributed within this range: ACM Digital Library resulted in approximately 60–64 papers per query, ScienceDirect approximately 60–62 papers per query, IEEE Xplore approximately 70 papers per query, and Scopus contributed approximately 40–54 papers per query.

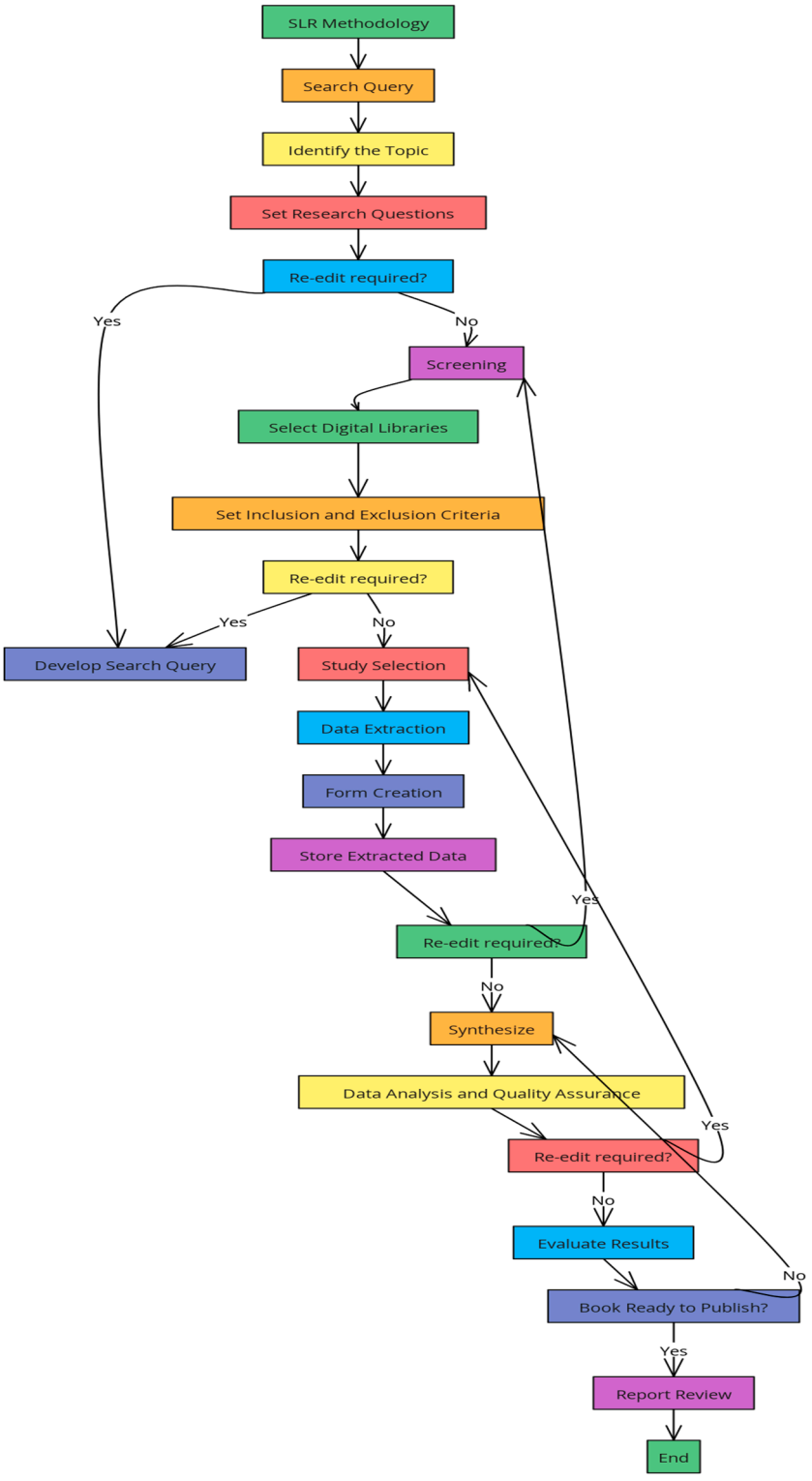

Figure 2. SLR methodology.

2.3. Data Extraction and Synthesis

This section outlines the method used to extract and analyze data from selected papers in order to address our research questions through a systematic literature review. The data extraction process relied on a form outlined in Table 3 and was carried out using Microsoft Excel Office 365 ProPlus spreadsheets.

Table 3. Collected Data Form.

SLR	Item	Description
1	Type	Publication Type (e.g., journal, conference).
2	Authors	Authors of the Article.
3	Year	Year of the Publication.
4	Title	Title of the Publication.
5	Source	Source of Publication (e.g., ACM Digital Library).
6	RQ1	Emerging crime threats on the Dark Net.
7	RQ2	Methods used to find the perpetrators of crimes on the Dark Net.

Figure 3 provides an overview of the data analysis process we used to address our research questions. Initially, we identified the relevant quality attributes from the chosen articles by following the selection criteria for each RQ. Next, depending on the RQ, we extracted the reasons behind the research and used thematic analysis to identify and extract the key themes from the articles.

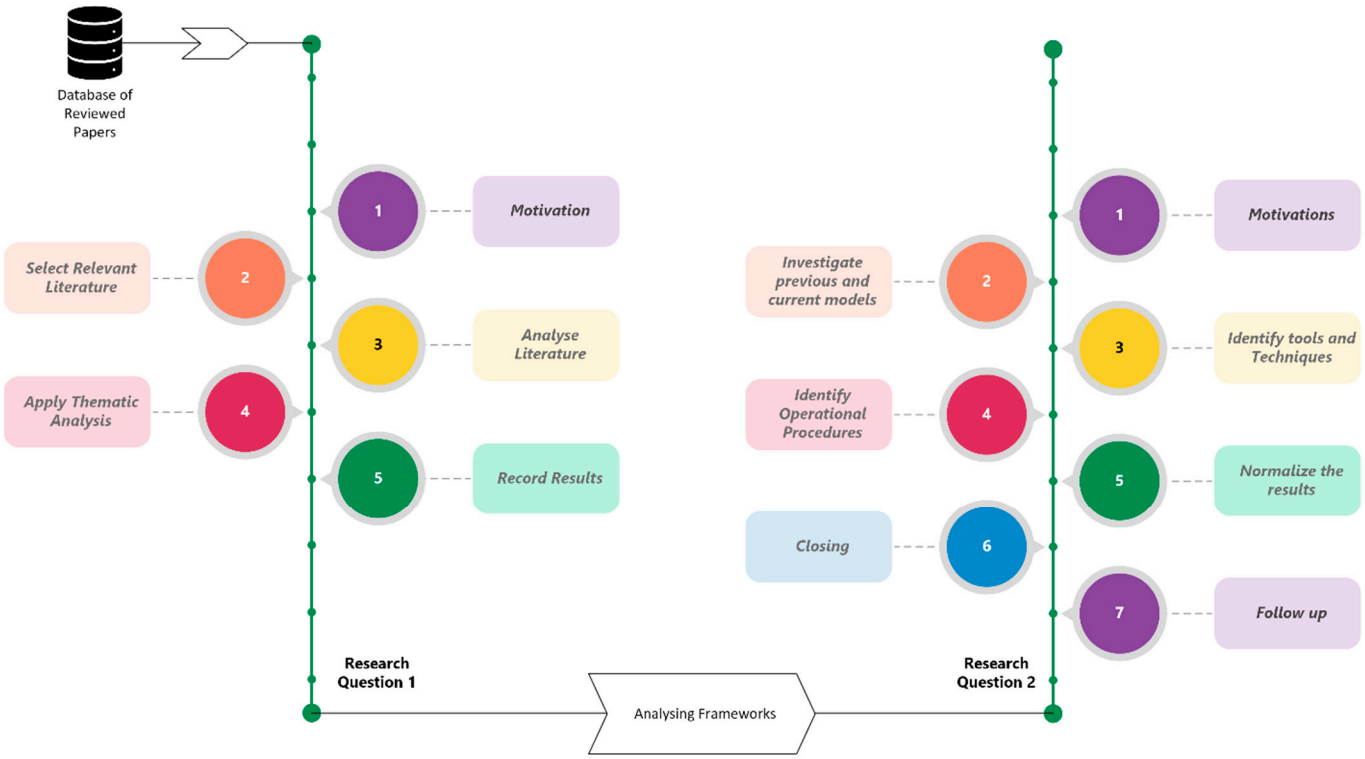

Figure 3. A Summary of the process for analyzing data.

The authors explored various motivations and frameworks previously employed, guided by distinct quality attributes and selection parameters. Through thematic analysis, they pinpointed recurring themes across the studies and applied qualitative data analysis with these themes to construct architectural frameworks documented in the literature. The emerging crime threats on the Dark Net identified in RQ1 are used as input for RQ2, revealing that the information gained from RQ1 is important for answering RQ2.

In addressing our second research question (RQ2), we delved into the data gathered from RQ1 to gain deeper insights into the architecture found within various literature sources, as illustrated in Figure 2. Our initial step in analyzing RQ2 data entailed extracting underlying motivations from the architectural summaries, aiming to discern the distinct features of the models employed across diverse methodologies. These features encompass aspects like data volume, practical application, and the efficacy of the models. Subsequent

thematic analysis allowed for the delineation of generalized models, thereby laying the groundwork for our architectural scrutiny. Upon pinpointing these generalized models, we proceeded to dissect the proposed models to catalog the assortment of tools and techniques utilized. Further thematic analysis of this phase yielded generalized methodologies, enriching our architectural analysis with detailed descriptions and examples.

3. Demographic Information

The demographic information section of this paper analyzes the distribution of reviewed papers based on primary studies, as shown in Table 4, publications categories, publication types, publications by year, main journals, interest over time, top queries, and countries.

Primary Studies

Table 4. Overview and contribution of the primary studies.

Authors	Paper	Contribution
[10]	Foundations and trends on Dark Net-related criminals in the last 10 years: a systematic literature review and bibliometric analysis	This paper makes a pioneering contribution by combining a systematic literature review with bibliometric analysis to map out the evolution of Dark Net-related crime research over the past decade, highlighting significant contributions from the Global South and identifying key areas for future study.
[3]	Classifying Illegal Activities on Tor Network Based on Web Textual Contents	This paper introduces "Dark Net Usage Text Addresses" (DUTA), a novel dataset of Dark Net domains that enables a systematic approach to categorize Tor hidden services. Through rigorous sampling and classification of Tor network addresses, our analysis reveals the efficacy of combining TFIDF word representation with logistic regression, achieving high cross-validation accuracy and macro F1 scores, providing a solid foundation for tools that could assist in identifying illicit activities on the Deep Web.
[16]	The shift of Dark Net illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence	This study utilizes temporal topic modeling and sentiment analysis on ClearNet forum data to uncover the enduring preference for Bitcoin among Dark Net market users until Monero's privacy enhancements in 2017 shifted the cryptocurrency landscape.
[17]	Threats from the Dark: A Review of Dark Web Investigation Research for Cyber Threat Intelligence	This review delineates the pivotal role of Dark Web content analysis in Cyber Threat Intelligence, providing an extensive survey of contemporary methodologies, tools, and challenges, and charting a course for future research in the domain.
[18]	Exploring Dark Web Crawlers: A Systematic Literature Review of Dark Web Crawlers and Their Implementation	This paper provides a comprehensive systematic literature review on Dark Web crawlers, detailing their common programming practices and tools, and introduces an innovative Tor-based crawling model, validated through experiments, to enhance the efficacy of digital investigations within anonymous communication networks.
[19]	Under and over the surface: A comparison of the use of leaked account credentials in the Dark and Surface Web	This study contrasts the criminal patterns of stolen account credentials' usage in the Surface Web with those on the Dark Web by deploying Gmail honey accounts, revealing distinct malicious behaviors in each realm and offering valuable insights into the dynamics of cybercrime across diverse web environments.
[20]	Recognition of service domains on TOR Dark Net using perceptual hashing and image classification techniques	This paper introduces DUSI, a unique image-based dataset of TOR services and presents a framework utilizing Perceptual Hashing and Bag of Visual Words to accurately identify various services on the TOR network through visual content, with Perceptual Hashing emerging as a highly effective approach for service detection.
[15]	Exploring and Mining the Dark Side of the Web	This talk explores the latest in Terrorism Informatics, highlighting the Dark Web project's advancements in web mining and analysis for tracking online terrorist activity, supported by a vast database of extremist content.

Table 4. *Cont.*

Authors	Paper	Contribution
[21]	Analysis of Hacking-Related Trade on the Dark Web	This study presents an exploratory analysis of the hacking trade in Dark Web marketplaces, revealing a profit-driven market that generated over USD 26 million, with the majority of products priced under USD 150, indicating the ease of access to cybercrime tools and the presence of a highly organized infrastructure.
[22]	A public policy perspective of the Dark Web	This paper provides an insightful overview of the Dark Web's history and current governmental interventions, offering policy recommendations to balance regulation with user values, critical for informed debate and effective global Dark Web policy development.
[23]	Criminal motivation on the dark web: A categorisation model for law enforcement	Introducing the Tor-use Motivation Model (TMM), this study presents a nuanced two-dimensional classification approach tailored for law enforcement, effectively bridging the gap between broad taxonomies and detailed criminal behavior analysis on the Dark Web.
[24]	SpyDark: Surface and Dark Web Crawler	SpyDark, an innovative tool, enables users to collect and analyze information from both the surface and Dark Web, leveraging crawler and NLP models to classify web pages by relevance based on user-defined queries.
[5]	The Dark Web and anonymizing technologies: Legal pitfalls, ethical prospects, and policy directions from radical criminology	This article examines the Dark Web's dual-edged nature, aiming to illuminate its complexities for policymakers and propose informed legal and ethical strategies to navigate its challenges and harness its potential responsibly.
[25]	Collective dynamics of Dark Web marketplaces	This study delves into the dynamics of Dark Web marketplaces, revealing how user migration to coexisting platforms following marketplace closures ensures the systemic resilience of the illicit trade ecosystem despite individual marketplace fragility.
[26]	Electronic Money Laundering: The Dark Side of Fintech: An Overview of the Most Recent Cases	This paper presents a systematic review of money laundering in the FinTech sector, examining common patterns, the European legal framework, and recent fraud cases to assess if economic behaviors align with legality and if FinTech tools can detect illicit activities.
[27]	Using social network analysis to prevent money laundering	This study leverages network analytic techniques on a factoring company's data, revealing that social network metrics can predict client risk profiles, with riskier entities engaging in larger, more frequent, and cross-sector transactions, often from peripheral network positions.
[28]	Power/freedom on the Dark Web: A digital ethnography of the Dark Web Social Network	This ethnographic essay investigates the Dark Web Social Network, highlighting its complex interplay of anonymity and sociality, its stance against illegal content, and the unique blend of techno-elitism, revealing a nuanced exploration of power and freedom within the digital underground.
[29]	A qualitative mapping of Dark Web marketplaces	This paper offers a comprehensive mapping of Dark Web marketplaces, examining their operational mechanisms and features through qualitative analysis, aiming to uncover vulnerabilities in the cyber security landscape and strategize their disruption.
[30]	Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web	The employment of hacking tools by law enforcement to track Dark Web users challenges the boundaries between criminal procedure and international law, as traditional surveillance methods become ineffective against anonymized online activities.
[31]	Automated Categorization of Onion Sites for Analyzing the Dark Web Ecosystem	This paper introduces ATOL, an advanced analysis tool within the LIGHTS infrastructure, designed for thematic assessment of Dark Web content, enhancing the capability to identify and monitor illicit sites through novel keyword discovery, classification, and clustering techniques, demonstrating significant performance gains in content categorization.

Table 4. *Cont.*

Authors	Paper	Contribution
[32]	Dark Web, Along With The Dark Web Marketing And Surveillance	This paper delves into the utilization of the Dark Web for criminal and terrorist activities, exploring how law enforcement agencies globally navigate and surveil the Dark Web to counteract these threats, while also discussing secure access methods and safety precautions for users.
[33]	Drug traders on a local Dark Web marketplace	This article employs habitus and way of life concepts to analyze the cultural and socioeconomic dimensions of Finnish Dark Web drug users' lives, using qualitative and quantitative analysis of forum posts from Sipulitori to reveal diverse drug-related lifestyles and inform future research on Dark Web forums.
[34]	A Framework for More Effective Dark Web Marketplace Investigations	This research presents an innovative analytical framework for Dark Web scraping using AppleScript, proving effective in a case study to unveil vendor identities and listings on a marketplace, offering significant insights for academics and investigators into the clandestine operations of Dark Web marketplaces.
[35]	Measuring Dark Web marketplaces via Bitcoin transactions: From birth to independence	This study tracks the evolution and transaction volumes of seven major Dark Web marketplaces, revealing their transition to more advanced anonymity tools by 2016 and the continuous user migration that sustains the Dark Web's illicit economy.
[36]	Beyond the Surface Web: How Criminals Are Utilizing the Internet to Commit Crimes	This research explores the dual-edged nature of online anonymity and cryptocurrencies, delving into their use in criminal activities and the ethical challenges faced by the criminal justice system, while questioning if digital forensics can meet the evolving demands of cyber investigations.
[37]	Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning	This paper proposes a novel approach using machine learning and natural language processing to extract and analyze valuable intelligence from Dark Web forums, aiming to enhance the prediction and prevention of increasingly sophisticated cyber-attacks.
[2]	Dark Web: A Web of Crimes	This paper provides a comprehensive overview of the Dark Web, detailing its features, advantages, disadvantages, and the browsers used to access it, while also highlighting the criminal activities it harbors, aiming to raise awareness and promote preventive measures against such illicit actions.
[6]	Understanding the Dark Web	This chapter delineates the distinctions and interrelations between the Surface Web, Deep Web, and Dark Web, explores the architecture and technologies of major Dark Nets like Tor, I2P, and Freenet, and addresses the complexities law enforcement agencies encounter in combating crime and terrorism within these anonymous realms.
[38]	Dark Web Markets	This chapter explores the distinctions and connections between the Surface Web, Deep Web, and Dark Web, delves into the infrastructure of key Dark Nets like Tor, I2P, and Freenet, and examines the impact of law enforcement on the Dark Web, highlighting the challenges of using anonymity technologies in the battle against online crime and terrorism.
[39]	Trust and Relationship Development Among Users in Dark Web Child Sexual Exploitation and Abuse Networks: A Literature Review From a Psychological and Criminological Perspective	This literature review delves into the dynamics of trust and relationship building within online networks on the Dark Web, focusing on the sexual exploitation and abuse of children, highlighting the complex interplay of social and technical factors that underpin these illicit communities.
[40]	A Crawler Architecture for Harvesting the Clear, Social, and Dark Web for IoT-Related Cyber-Threat Intelligence	This study introduces a cutting-edge crawling architecture that efficiently harvests cyber-threat intelligence from diverse web layers, employing machine learning and statistical language models to prioritize relevant security information, showcasing its potential through an open-source toolkit and crowdsourced evaluation.

Table 4. *Cont.*

Authors	Paper	Contribution
[41]	Money talks money laundering choices of organized crime offenders in a digital age	This study delves into the financial strategies of organized crime, highlighting a universal preference for cash across both traditional and cybercrime, while noting a distinct utilization of financial innovations like cryptocurrencies primarily within IT-related criminal activities.
[42]	A Qualitative Analysis of Illicit Arms Trafficking on Dark Net Marketplaces	This qualitative study explores the landscape of illegal arms trafficking on the Dark Web, utilizing a custom crawler to analyze data from ten marketplaces, revealing a well-organized trade in military-grade weapons and corroborating previous institutional reports on the ease of access and variety of firearms available.
[43]	Mining Key-Hackers on Dark Web Forums	This study introduces a novel approach for identifying key hackers in Dark Web forums using a blend of content, social networks, and seniority analyses, complemented by a reputation-based validation method, demonstrating that a hybridized model enhances key-hacker detection and can be generalized across different forums.
[7]	Anonymity Services Tor, I2P, JonDonym: Classifying in the Dark	This paper demonstrates the effectiveness of machine-learning classifiers in distinguishing between different anonymity networks (Tor, I2P, JonDonym) and identifying the specific applications generating encrypted traffic, achieving remarkable accuracies using only statistical features from a 2017 public dataset.
[44]	Dark Web research: Past, present, and future trends and mapping to sustainable development goals	This bibliometric analysis of Dark Web research over the past decade identifies four key areas of focus—network security, cybercrime and cryptography, machine learning and AI, drug trafficking and cryptomarkets—while highlighting the challenge it poses to achieving the UN's SDGs, particularly SDG 16, and underscores the need for interdisciplinary approaches to develop effective countermeasures.
[45]	Artificial Cyber Espionage-Based Protection of Technological Enabled Automated Cities Infrastructure by Dark Web Cyber Offender	This work examines the evolving landscape of cybersecurity in the era of IoT, highlighting the dual use of technology by both security experts and infiltrators, and explores advanced strategies for protecting against cyber threats, emphasizing the critical role of identifying and countering digital criminals, particularly through the Dark Web.
[46]	Dark Web—Onion Hidden Service Discovery and Crawling for Profiling Morphing, Unstructured Crime, and Vulnerabilities Prediction	This research delves into the underbelly of the Dark Web, highlighting its role as a hub for various illegal activities, and outlines methodologies for crawling and analyzing its content to understand the patterns and behaviors of cybercriminals and terrorists, thereby shedding light on the challenges faced by law enforcement in combating these hidden crimes.
[11]	A general and modular framework for Dark Web analysis	This study introduces a versatile and scalable framework for Dark Web analysis, employing a microservice architecture with Docker Swarm, Kafka, ELK Stack, and PostgreSQL, successfully scraping over 84,000 unique onion domains, showcasing its efficacy in integrating diverse analytical workflows.
[47]	A Survey of Challenges Posed by the Dark Web	This study proposes a flexible and scalable framework for Dark Web analysis, demonstrating its efficacy in scraping over 84,000 unique onion domains.
[9]	An Anonymity Vulnerability in Tor	This paper introduces novel Trapper Attacks that exploit vulnerabilities in Tor to deanonymize user activities, demonstrating their effectiveness in real-world Tor networks with a success rate exceeding 99% and minimal false positives.
[48]	Characterizing Activity on the Deep and Dark Web	This paper investigates the Deep and Dark Web (d2web), where illicit activities thrive, using a large dataset of forum messages spanning over a year. By employing topic modeling techniques like LDA and a non-parametric HMM, it uncovers hidden patterns and similarities across forums, facilitating the identification of anomalous events.
[49]	A survey on technical threat intelligence in the age of sophisticated cyber attacks	This paper elucidates the nuances of threat intelligence, particularly focusing on Technical Threat Intelligence (TTI), while addressing challenges in sharing and standardizing threat information to enhance security efficacy.

Table 4. *Cont.*

Authors	Paper	Contribution
[50]	Dark web in the dark: Investigating when transactions take place on cryptomarkets	This study investigates the temporal patterns of illegal transactions on leading cryptomarkets, revealing heightened activity during night-time hours and on weekdays, particularly Mondays through Wednesdays. Additionally, it suggests that law enforcement operations like Operation Onymous may not significantly disrupt cryptomarket activity or alter transaction patterns in the short term.
[51]	A Crime Script Analysis of Child Sexual Exploitation Material Fora on the Dark Web	This study employs a crime script analysis to unravel the sequential steps involved in Child Sexual Exploitation Material (CSEM) crimes within Dark Web communities, shedding light on the intricate process, from accessing illicit fora to post-activity behaviors. The findings underscore the challenges posed by Dark Web platforms in facilitating and shaping the commission of such crimes, providing insights for targeted law enforcement interventions.
[52]	Anonymous Trading on the Dark Online Marketplace: An Exploratory Study	This chapter delves into the realm of anonymous trading on the Dark Web, leveraging the Silkroad 2.0 dataset to dissect the nuances of illicit e-commerce. Through thematic analysis of drug-related discourse on Twitter, it unveils the global scope of illegal trading activities and underscores the susceptibility of adolescent populations to social media drug trafficking.
[53]	Law Enforcement and Digital Policing of the Dark Web: An Assessment of the Technical, Ethical, and Legal Issues	This chapter delves into the intricate challenges faced by law enforcement agencies in policing the Dark Web, highlighting the critical need for enhanced cyber threat intelligence, ethical considerations, and cross-border collaboration. It underscores the imperative of maintaining a delicate balance between law enforcement efforts and individual civil liberties, emphasizing the importance of deploying unpredictable policing techniques to effectively combat digital crime.
[54]	Terrorist Migration to the Dark Web	This paper explores recent trends in terrorist utilization of the Dark Web, highlighting its role in facilitating their operations while evading detection and law enforcement efforts.
[55]	Monitoring Product Sales in Dark Net Shops	This paper proposes a monitoring approach for tracking product sales on the Dark Net, leveraging anonymity networks like Tor and cryptocurrencies such as Bitcoin. By collecting Bitcoin addresses and product data from hidden services on Tor, the study aims to analyze blockchain transactions corresponding to specific sales in these Dark Net shops, offering insights into criminal activities while presenting opportunities for law enforcement and researchers alike.
[56]	Surfacing collaborated networks on the Dark Web to find illicit and criminal content	This paper addresses the proliferation of illegal activities on the Tor network, highlighting challenges in automated monitoring and the development of a modified web crawler termed the “Dark Crawler” to navigate the Dark Web. Initial findings reveal the presence of extremist and terrorist content and its interconnectedness, shedding light on the facilitation of Dark Web crimes by popular websites owithin the Dark Web ecosystem.
Our study	Weaponization of the Growing Cybercrimes Inside the Dark Net: The Question of Detection and Application	This study fills significant gaps in the existing literature by providing a comprehensive review of the weaponization of cybercrimes on the Dark Web. Unlike previous studies that primarily focused on categorizing illegal activities or analyzing specific detection methodologies, our research holistically examines the lifecycle of these cybercrimes from their weaponization to their detection and impact assessment. By synthesizing insights from 88 relevant articles and incorporating the latest data from 2024 and backwards, we address the lack of comprehensive evaluations found in works like “Foundations and Trends on the Dark Net-Related Criminals in the Last 10 Years” and “Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence.” Our study provides actionable recommendations for policymakers, cybersecurity professionals, and law enforcement agencies to enhance efforts in combating weaponized cybercrimes on the Dark Web, thus proposing future measures for improved crime monitoring and locating technologies.

In positioning our study within the existing literature on Dark Web cybercrimes, we aim to build on and expand the current understanding of this complex and evolving field. Previous studies, such as "Foundations and Trends in the Dark Net-Related Criminals in the Last 10 Years" by Author [10], have provided a comprehensive bibliometric analysis that maps out the evolution of Dark Net-related crime research, highlighting significant contributions from various regions and identifying future study areas. This foundational work sets the stage for more targeted investigations into specific aspects of Dark Web activities.

Our study distinguishes itself by focusing explicitly on the weaponization of cybercrimes within the Dark Web, an area that has seen growing concern but lacks comprehensive exploration. While studies like "Classifying Illegal Activities on Tor Network Based on Web Textual Contents" by Author [3] have introduced systematic approaches to categorize hidden services and understand illicit activities through datasets like DUTA, they primarily address classification and detection methodologies. Our research goes a step further by examining how these cybercrimes are being weaponized and used to launch attacks against various targets, including individuals, businesses, and governments.

Moreover, existing literature such as "Threats from the Dark: A Review Over Dark Web Investigation Research for Cyber Threat Intelligence" emphasizes the role of Dark Web content analysis in cyber threat intelligence, surveying contemporary methodologies and challenges. Our study contributes to this discourse by evaluating the effectiveness of these methodologies, specifically in the context of detecting and mitigating weaponized cyber threats. We explore technical tools such as blockchain analysis and Dark Net crawlers, and the role of human intelligence, thus providing a more integrated approach to understanding and combating these threats.

Additionally, research like "Exploring Dark Web Crawlers: A Systematic Literature Review of Dark Web Crawlers and Their Implementation" has detailed the implementation and efficacy of crawling models for digital investigations. We extend this by assessing the application of these tools in real-world scenarios, studying the impact of cyber-attacks facilitated through the Dark Web and the subsequent challenges faced by law enforcement.

Our unique contribution lies in the holistic examination of the lifecycle of Dark Web cybercrimes, from their weaponization and execution to detection and impact assessment. By synthesizing insights from 88 relevant articles and incorporating the latest data from 2024, we address existing gaps and propose future measures for more effective crime monitoring and mitigation strategies. This approach not only enriches the current body of knowledge but also provides actionable recommendations for policymakers, cybersecurity professionals, and law enforcement agencies to enhance their efforts in combating the growing threat of weaponized cybercrimes on the Dark Web.

3.1. Types of Publications

The bar chart in Figure 4 presents the distribution of various publication types for the 88 studies included in our analysis. Journals lead significantly, with 47 publications, indicating a strong preference for disseminating research through this medium. Conferences come next, with 21 entries, suggesting that these are also a popular avenue for sharing information, possibly due to the interactive nature of these events. Book chapters, with 14 publications, show a moderate level of contribution, which might imply a focus on comprehensive coverage of topics in edited volumes. Primary handbooks, industry reports, government reports, online websites, and symposiums have the least representation, with 1–2 publications each. This could reflect a more niche audience or a more selective dissemination approach for specialized or official content.

The high number of journal articles reflects the academic nature of research related to the Dark Web and the use of scholarly journals as the primary dissemination outlet. Conference papers are also a common type of publication in the field of computer science and related fields. The lower number of book chapters and other publications suggest that research related to the Dark Web is primarily disseminated through academic channels.

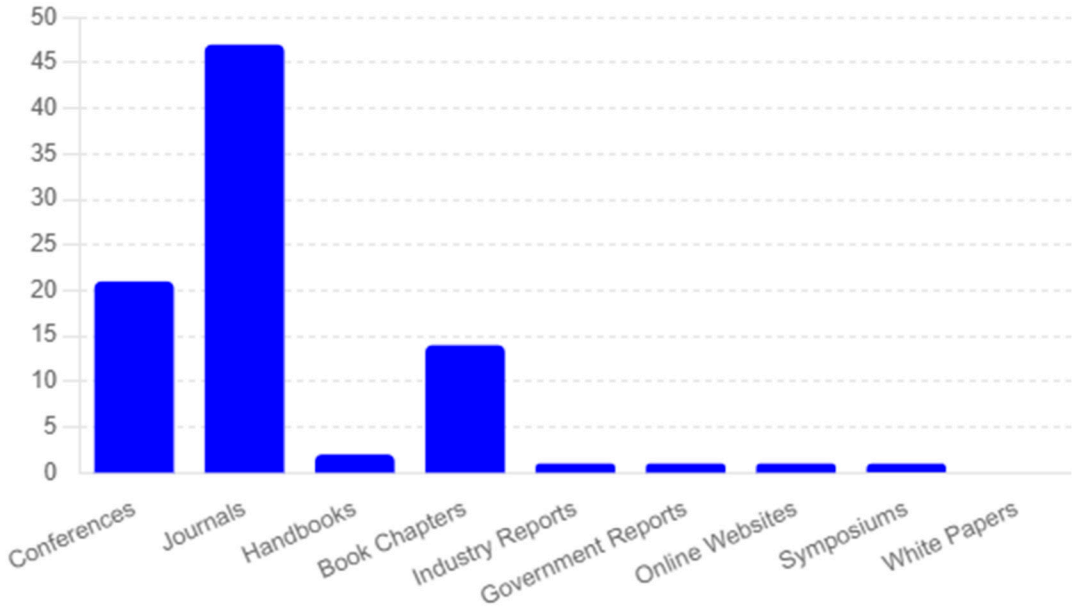

Figure 4. Distribution of publications.

3.2. Publications by Year

The reviewed papers present a comprehensive view of the research output related to the Dark Web from 2011 to 2023. Figure 5 reveals a fluctuating yet generally upward trend in publications, with notable peaks in certain years. The years 2018, 2021, and 2023 stand out, indicating periods of heightened scholarly activity and possibly reflecting responses to evolving challenges in cybersecurity and Dark Web phenomena. The steady increase in publications, particularly from 2018 onwards, suggests a growing recognition of the complexities and threats associated with the Dark Web, driving academic and practical interests in exploring, understanding, and mitigating related cybersecurity issues. This trend underscores the dynamic nature of cyber threats and the critical need for continuous research and innovation in digital forensics, cybersecurity measures, and law enforcement strategies to combat illicit activities on the Dark Web.

The pie chart in Figure 6 visualizes the distribution of publication categories based on the entire list. It clearly illustrates the emphasis on "Cybersecurity and Dark Web Analysis" as the dominant category, followed by "Illegal Activities and Law Enforcement", "Technical and Methodological Approaches", and "Policy and Ethical Considerations".

The high number of publications related to cybercrime reflects the significant threat that cybercrime poses to individuals, organizations, and society as a whole. As the Dark Web provides a platform for cybercriminals to conduct their activities anonymously, there is a need for research to understand the nature of cybercrime and ways to combat it.

Drug trafficking is another significant topic related to the Dark Web, with a quarter of the reviewed papers addressing this issue. The Dark Web provides a platform for drug dealers to sell their products anonymously, making it challenging for law enforcement agencies to track down and prosecute them. Research in this area is essential to develop effective strategies to combat drug trafficking and its associated harms.

Anonymity was also a prevalent topic in the reviewed papers, with 21% of the publications addressing this issue. The Dark Web provides anonymity to its users, making it easier for criminals to operate without fear of being caught. Research in this area is important in order to understand the challenges of tracking and identifying criminals on the Dark Web and to develop effective strategies to combat their activities.

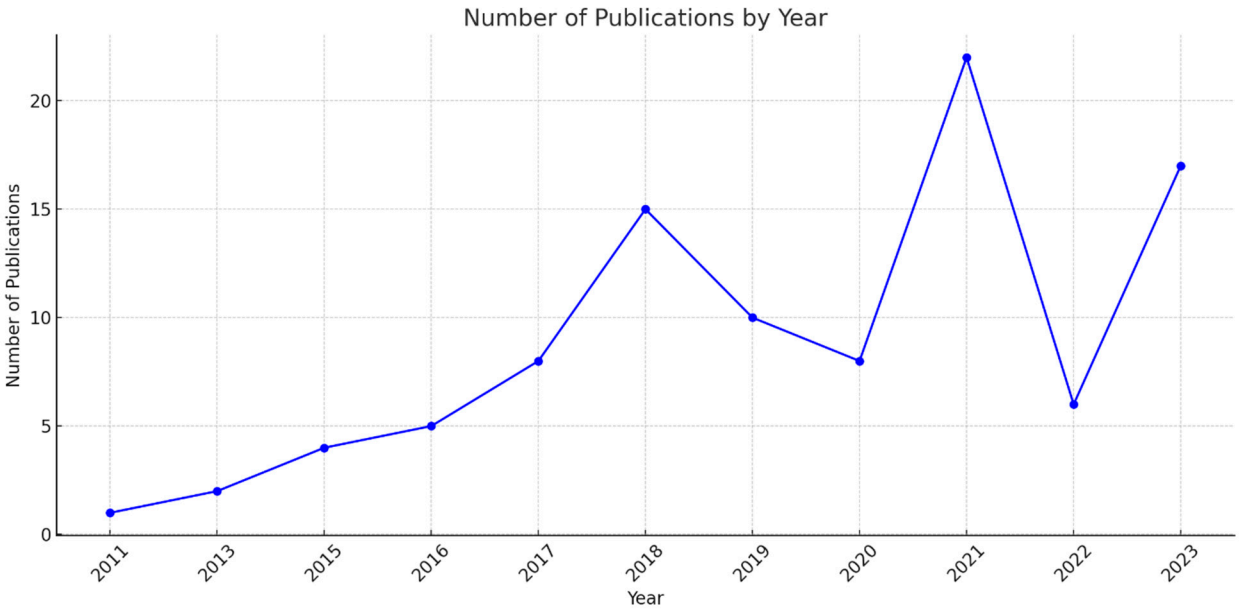

Figure 5. Number of publications by year.

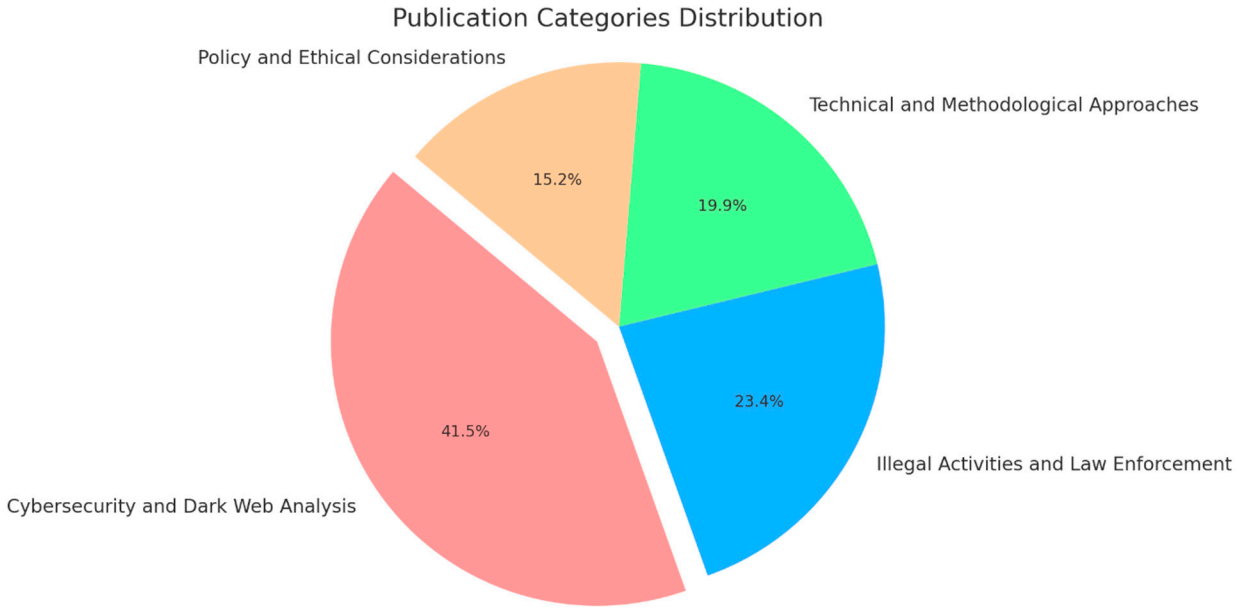

Figure 6. Publication categories.

3.3. Publication Sources and Countries

Eighty-eight papers have been analyzed thoroughly to select top publication sources in the field of the Dark Web based on the most cited publications. The top publication sources for journal articles on the topic of the "Dark Web" and the countries where these publications originated are shown in Figure 7 and Table 5.

Figure 7 presents a comparative analysis of public interest in "Dark Net" versus "Cyber Crime" over an approximately one-year period, from March 2023 to February 2024. The data indicate a markedly higher and consistent interest in "Cyber Crime", which hovers around the 75% interest level without significant fluctuation, suggesting it is a persistent topic in public discourse. Conversely, the "Dark Net" garners considerably less interest, averaging below 25% throughout the same period, indicating a relatively stable but low engagement with this topic. The steady interest in "Cyber Crime" might reflect ongoing societal concerns, continuous media coverage, or a stable rate of incidents being reported.

The much lower profile of the "Dark Net" in public interest metrics could imply that, while it is acknowledged as a part of cyber security discussions, it does not resonate or is not as well understood by the public as the broader issues encompassed by "Cyber Crime".

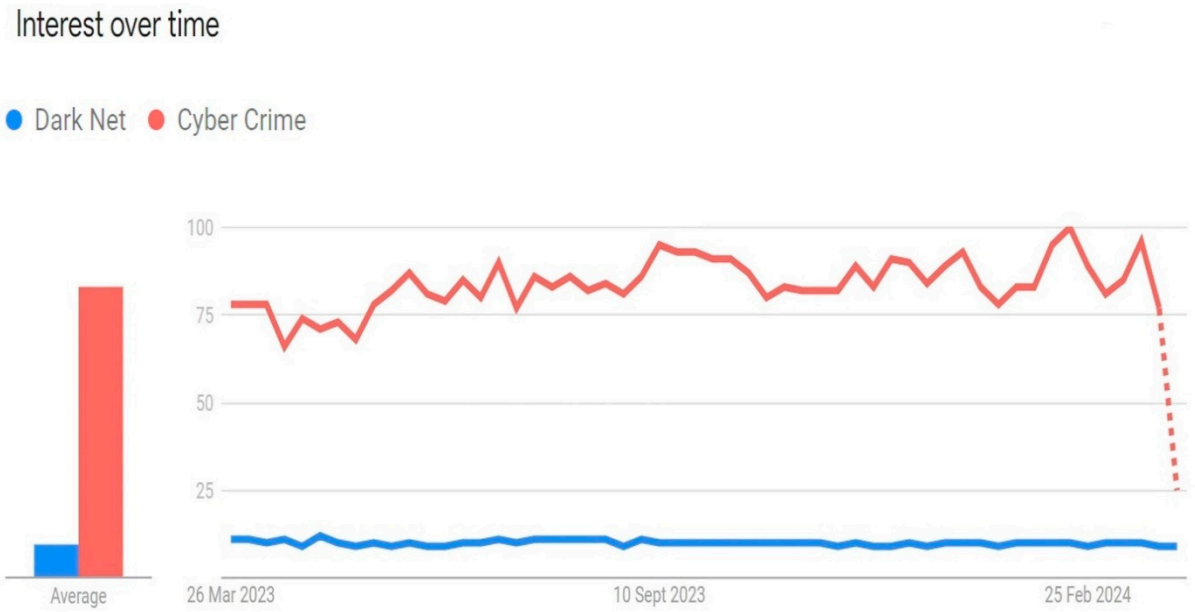

Figure 7. Interest over time (March 2023–February 2024).

Table 5. Top publication sources and countries.

Journal	Country
Journal of Strategic Security	United States
Frontiers in Computer Science	Switzerland
Forensic Science International: Digital Investigation	United Kingdom
Journal of Computer Networks and Communications	Egypt
Security Journal	United States
Computers in Human Behavior	United Kingdom
Crime Science	United Kingdom
Journal of Cyber Policy	United Kingdom
Crime, Law, and Social Change	Netherlands
Scientific Reports	United Kingdom
Expert Systems with Applications	United Kingdom
Journal of Cybersecurity and Privacy	Switzerland
Deviant Behavior	United Kingdom
Trauma, Violence, & Abuse	United Kingdom
Journal of Information Security and Applications	United Kingdom
Computer Fraud and Security	United Kingdom
Heliyon	Netherlands
Journal of Economic Criminology	United Kingdom
Computers and Security	United Kingdom

In Figure 8, we see a world map depicting the regional interest in "Dark Net" (blue) and "Cyber Crime" (red). The intensity of the colors represents the relative level of interest in these topics across different regions. From a glance at the map, it is evident that "Cyber

Crime" has a more substantial presence globally, indicated by the widespread red coloring. Notably, North America, parts of Europe, and some regions in Asia exhibit a higher interest in "Cyber Crime".

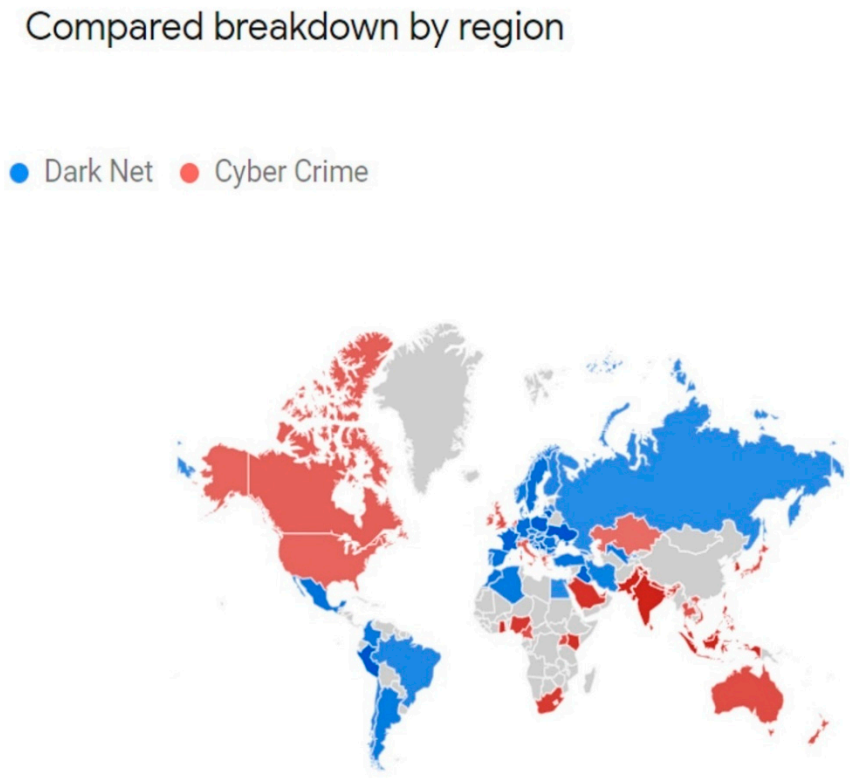

Figure 8. Interest by regions and countries.

On the other hand, the "Dark Net" shows a much more limited geographical footprint in terms of public interest. Only a few regions are marked in blue, suggesting that there are specific areas where "Dark Net" garners attention, although it is significantly less than that for "Cyber Crime".

The contrast in color saturation between the two topics suggests that while "Cyber Crime" is a globally recognized issue, the "Dark Net" is either less understood, less reported, or perhaps of interest only in particular contexts or regions.

This visual comparison provides valuable insight into how different regions prioritize these aspects of cybersecurity and can be indicative of regional awareness, media focus, or the prevalence of related incidents. It may also reflect cultural and legislative differences in the perception and handling of cyber-related threats. Related queries: top 10 queries, see the figure below.

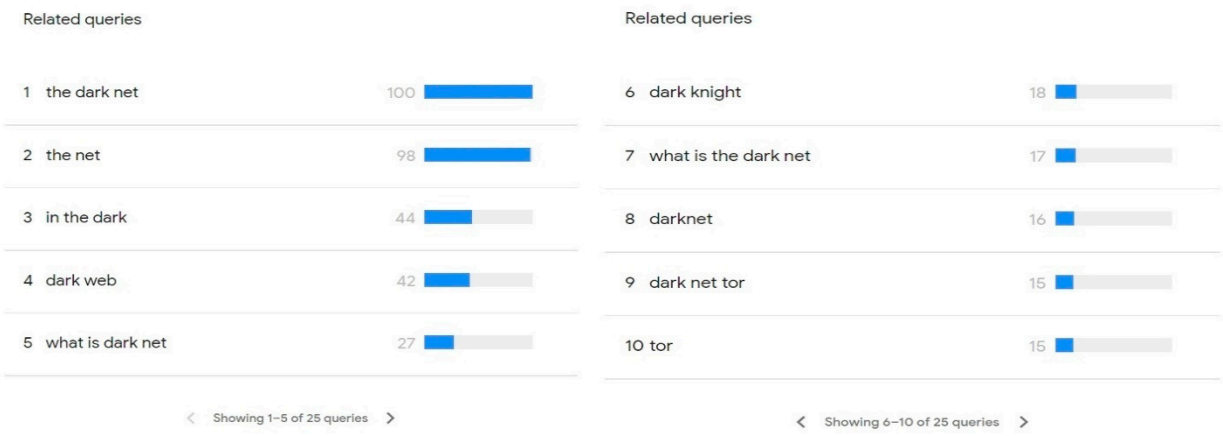

Figure 9 presents a radar chart that illustrates the market share distribution among the largest Dark Web marketplaces based on the primary studies and interest analysis up to 2024. The data show the dominance of specific marketplaces in terms of their share of the total market. The key insights from this figure are as follows:

BlackSprut Market: Holding the largest market share at 28%, BlackSprut Market is a significant player within the Dark Web ecosystem. This dominance indicates its popularity and the volume of transactions it handles, making it a critical focus for law enforcement and cybersecurity professionals.

Mega Darknet Market: With a 22% market share, Mega Darknet Market is the second-largest marketplace. Its substantial share suggests a high level of trust and user engagement, highlighting its importance in the illegal online economy.

OMG! OMG! Market: This marketplace accounts for 17% of the market share, making it the third largest. The significant share indicates that it is a key player, particularly in certain types of transactions or products that may differentiate it from competitors.

Solaris Market: Solaris Market holds a 13% market share, placing it among the top four marketplaces. This share suggests a robust presence and likely specialization in certain illegal goods or services.

ASAP Market: With a 7% market share, ASAP Market is smaller compared to the top four but still plays a notable role in the Dark Web economy. This market likely caters to niche segments or specific types of transactions.

Other Marketplaces: The remaining 13% of the market is distributed among various smaller marketplaces. This fragmentation indicates the existence of numerous platforms catering to specific or emerging needs within the Dark Web community.

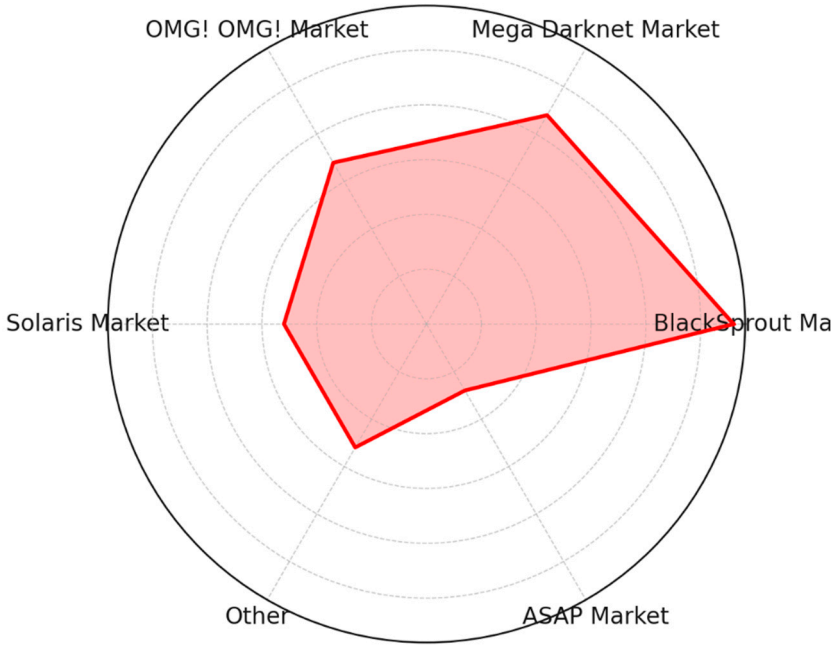

Figure 9. Largest Dark Web marketplaces.

4. Findings

This section aims to provide answers to the two research questions and discuss the findings obtained from our systematic review of the literature. The first research question (RQ1) is focused on identifying the emerging threats in Dark Web crimes, which is addressed in Section 1. Sections 4.1.1–4.1.6 provide an overview of the threats that have arisen from criminal activities on the Dark Web. The second research question (RQ2) is focused on analyzing the various techniques used to track criminals on the Dark Web. This is discussed in Section 2, with analyses of the methods and techniques used against these

threats in Sections 4.2.1–4.2.6. Finally, Section 4.3 presents a summative evaluation of the contents of the 88 studies that were extracted and their contributions.

4.1. Activities on the Dark Web

The Dark Web is known to host various criminal activities and threats, as shown in Figure 10, including the following:

1. **Illegal Marketplaces**: The Dark Web is notorious for illegal marketplaces that sell a wide range of illicit goods and services, such as drugs, weapons, counterfeit documents, stolen data, and hacking tools.
2. **Cybercrime-as-a-Service**: Criminals offer various hacking services on the Dark Web, such as DDoS attacks, malware creation, and phishing campaigns for a fee.
3. **Identity Theft**: Criminals can buy or sell stolen personal information, such as credit card numbers, social security numbers, and passwords, on the Dark Web.
4. **Child Exploitation**: The Dark Web hosts illegal websites that exploit children, such as child pornography and human trafficking.
5. **Money Laundering**: Criminals use the Dark Web to launder money by exchanging cryptocurrencies or converting illegal funds into legitimate assets.
6. **Espionage**: Nation-states and other actors can use the Dark Web to conduct espionage activities, such as stealing sensitive data or launching cyber-attacks on critical infrastructure.

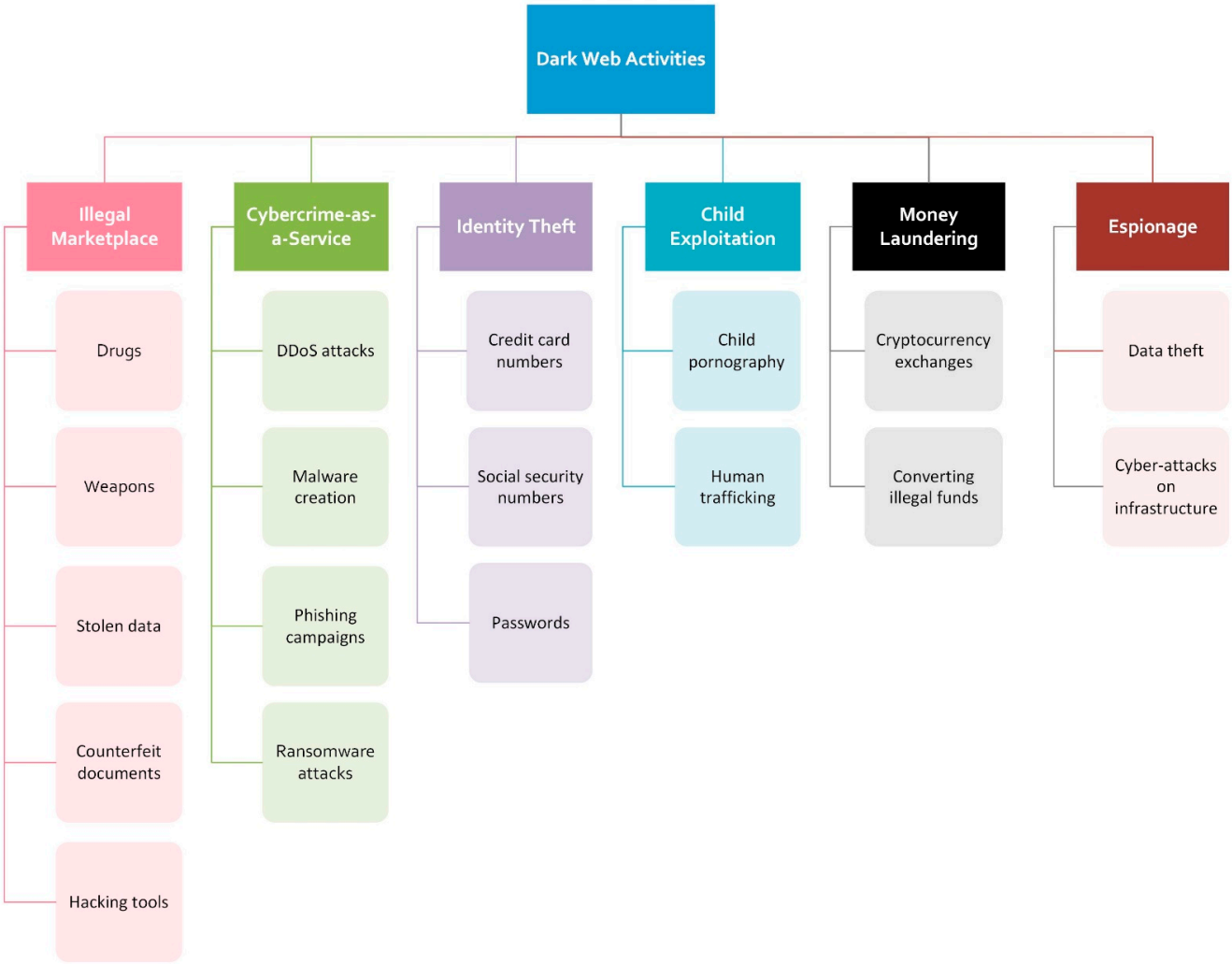

Figure 10. Activities on the Dark Web.

4.1.1. Illegal Marketplaces

Illegal marketplaces on the Dark Web are online platforms that allow individuals to buy and sell illegal goods and services anonymously [35]. These marketplaces operate on hidden servers, often using encryption and other security measures to avoid detection by law enforcement agencies [52]. The anonymity and lack of regulation on the Dark Web make these marketplaces a hotbed for illegal activities, including drug trafficking, weapons sales, and the sale of stolen data.

The Dark Web is notorious for being a hub for illegal activities, including the buying and selling of illicit goods and services. Here are some statistics regarding the illegal marketplaces on the Dark Web:

- The global illegal drug market is estimated to be worth around USD 360 billion annually, and a significant portion of this market is conducted through Dark Web marketplaces [57,58].
- According to a report by Chainalysis, the total revenue generated from Dark Net marketplaces in 2020 was USD 1.7 billion, with most transactions involving drugs, fraud, and stolen data [25].
- The same report found that the Dark Net market revenue from cryptocurrencies increased by over 60% in 2020, with Bitcoin being the most used cryptocurrency for transactions on these marketplaces.
- The most sold drugs on Dark Net marketplaces include marijuana, cocaine, and opioids like fentanyl [59].

Drug Marketplaces

Drug marketplaces are some of the most well-known illegal marketplaces on the Dark Web [34]. These marketplaces allow individuals to buy and sell a wide range of illicit substances, from marijuana and cocaine to prescription drugs and opioids [60]. Many drug marketplaces operate using the same model as legitimate e-commerce platforms, with vendors listing their products and buyers leaving reviews and ratings. Some marketplaces even offer customer support services and money-back guarantees.

While drug marketplaces on the Dark Web have been around for years, law enforcement agencies around the world have been cracking down on them in recent years [22]. For example, in 2019, the US Department of Justice shut down two of the largest drug marketplaces on the Dark Web, AlphaBay and Hansa Market, and arrested several of their administrators and vendors [61].

Weapons Marketplaces

Weapons marketplaces are another type of illegal marketplace that can be found on the Dark Web. These marketplaces offer a range of firearms, explosives, and other weapons to buyers around the world. Some weapons marketplaces even offer tutorials on how to make homemade explosives and firearms, making it easier for individuals to create their own weapons [29]. Because weapons are highly regulated in most countries, many buyers and sellers on weapons marketplaces are criminals or individuals who would not be able to purchase weapons legally [42]. As a result, these marketplaces are a significant concern for law enforcement agencies around the world.

Stolen Data Marketplaces

Stolen data marketplaces are another type of illegal marketplace on the Dark Web. These marketplaces offer a range of stolen data, including credit card numbers, social security numbers, and login credentials. This data can be used for identity theft, fraud, and other criminal activities [2]. Stolen data marketplaces are often used by cybercriminals who want to monetize the data they have stolen through hacking or phishing attacks. Buyers can purchase this data using cryptocurrency, making it difficult for law enforcement agencies to track and identify the buyers and sellers [23].

Other Illegal Marketplaces

In addition to drug, weapons, and stolen data marketplaces, there are many other types of illegal marketplace on the Dark Web [55]. For example, there are marketplaces that offer counterfeit goods, such as fake designer handbags and watches [21]. There are also

marketplaces that offer hacking services, such as the ability to hack into someone's social media account or steal their personal information [32,46].

The existence of these illegal marketplaces on the Dark Web presents significant challenges for law enforcement agencies around the world [33,62]. Because these marketplaces operate anonymously and use sophisticated encryption and security measures, it can be difficult to track down and identify the individuals involved. Furthermore, the use of cryptocurrency for transactions makes it difficult to follow the money trail.

However, law enforcement agencies have had some success in cracking down on illegal marketplaces on the Dark Web. In addition to shutting down AlphaBay and Hansa Market, law enforcement agencies have arrested and prosecuted many individuals involved in illegal marketplaces on the Dark Web. This includes both the administrators of these marketplaces and the vendors who sell illegal goods and services.

In conclusion, illegal marketplaces on the Dark Web pose significant challenges for law enforcement agencies and present a significant threat to individuals around the world. These marketplaces offer a range of illegal goods and services, from drugs and weapons to stolen data and counterfeit goods.

4.1.2. Cybercrime-as-a-Service

Cybercrime-as-a-Service (CaaS) is a model in which cybercriminals sell their hacking tools, services, and expertise to other criminals in exchange for payment [63]. This model has become increasingly popular on the Dark Web, where buyers and sellers can remain anonymous and conduct transactions using cryptocurrency [64]. CaaS has made it easier for individuals with little to no technical expertise to launch cyber-attacks, increasing the overall threat of cybercrime [65].

CaaS has become a thriving industry on the Dark Web, with a range of services available for purchase [66]. Some of the most popular services include Distributed Denial of Service (DDoS) attacks, ransomware, and phishing attacks [67]. For example, a buyer can purchase a DDoS attack service, which will flood a target website with traffic, causing it to crash. Similarly, a buyer can purchase a ransomware service, which will encrypt a victim's files and demand payment in exchange for the decryption key [68].

One of the key benefits of CaaS is that it makes cybercrime more accessible to individuals with little to no technical expertise [66]. In the past, launching a cyber-attack required a significant amount of knowledge and skill [69]. However, with CaaS, individuals can simply purchase the tools and services they need to launch an attack. This has led to a significant increase in the number of cyber-attacks launched each year and has made it more difficult for law enforcement agencies to track down and prosecute cybercriminals [49].

Another benefit of CaaS is that it allows cybercriminals to remain anonymous [70]. Transactions are conducted using cryptocurrency, making it difficult for law enforcement agencies to track down the buyers and sellers involved [16]. This anonymity also makes it easier for cybercriminals to evade detection and avoid prosecution.

Despite the benefits of CaaS, it is important to note that it presents a significant threat to individuals and organizations around the world. Cyber-attacks launched using CaaS can cause significant damage, including financial loss, data theft, and reputational damage. In addition, CaaS has made it easier for nation-states and other state-sponsored actors to launch cyber-attacks against other countries, further increasing the overall threat of cyber warfare.

According to a report by cybersecurity firm, Trend Micro, the underground market for Cybercrime-as-a-Service (CaaS) continued to grow in 2021, with new players entering the market and existing players expanding their offerings [71]. The most common types of CaaS offerings on the Dark Web in 2021 were malware-as-a-service, ransomware-as-a-service, and DDoS-as-a-service, according to a report by cybersecurity firm, Armor.

To combat the threat of CaaS, law enforcement agencies around the world are taking a range of measures. One approach is to target the marketplaces and forums where CaaS is sold. By shutting down these marketplaces and arresting the individuals involved, law

enforcement agencies can disrupt the supply chain of cybercrime and make it more difficult for criminals to launch attacks.

Another approach is to raise awareness of the threat of CaaS among individuals and organizations. This includes educating individuals on how to protect themselves from cyber-attacks and how to recognize the signs of a potential attack. It also includes working with organizations to improve their cybersecurity measures, such as implementing multi-factor authentication and regularly backing up data.

In conclusion, Cybercrime-as-a-Service has become a significant threat on the Dark Web, making it easier for individuals with little to no technical expertise to launch cyber-attacks. This model has led to a significant increase in the number of cyber-attacks launched each year and has made it more difficult for law enforcement agencies to track down and prosecute cybercriminals. To combat the threat of CaaS, law enforcement agencies are taking a range of measures, including targeting the marketplaces where CaaS is sold and raising awareness of the threat among individuals and organizations. However, the threat of CaaS remains significant, and individuals and organizations must remain vigilant in protecting themselves against cyber-attacks.

4.1.3. Identity Theft

Identity theft has become a lucrative business on the Dark Web, where personal information is bought and sold on a regular basis [72]. The industry of stealing identities has grown significantly in recent years, with cybercriminals using a range of tactics to obtain personal information that they can then sell to others on the Dark Web [73].

According to a report by the Identity Theft Resource Center (ITRC), there were 1108 reported data breaches in the US alone in 2020, which exposed over 300 million records [74]. Many of these data breaches lead to sensitive information, such as names, dates of birth, social security numbers, and financial information, being sold on the Dark Web.

One of the most common tactics used by cybercriminals to steal identities is phishing [19]. This involves sending emails that appear to be from legitimate sources, such as banks or other financial institutions, in an attempt to trick individuals into providing their personal information. These emails may contain links to fake websites that look like the real thing, or they may contain attachments that install malware on the victim's computer.

Another tactic used by cybercriminals is malware, which can be installed on a victim's computer without their knowledge [37]. Once installed, the malware can record keystrokes, capture screenshots, and steal login credentials, among other things. This information can then be used to gain access to the victim's accounts, steal their money, or commit other fraudulent activities.

Data breaches are another common way that personal information is stolen [75]. Cybercriminals will target companies that store large amounts of personal data, such as banks, retailers, and healthcare providers. Once they gain access to the company's database, they can steal the personal information of thousands or even millions of individuals [48]. Once cybercriminals have obtained personal information, they can sell it on the Dark Web to other criminals looking to commit fraud or other illegal activities. The price for this information can vary depending on the type and amount of data being sold. For example, a credit card number may sell for a few dollars, while a complete identity profile, including a social security number, date of birth, and address, can sell for hundreds of dollars.

The impact of identity theft can be devastating for victims, who may have their credit ruined, their savings wiped out, and their reputations damaged. It can take years to recover from the effects of identity theft, and many victims may never fully recover.

In conclusion, the industry of stealing identities on the Dark Web is a major problem that continues to grow. Cybercriminals are using increasingly sophisticated tactics to obtain personal information, and the personal data of millions of individuals is being bought and sold on the Dark Web every day. Protecting nations and organizations from identity theft requires constant vigilance and a proactive approach to online security.

4.1.4. Child Exploitation

Child exploitation on the Dark Web takes many forms. One of the most common forms is the distribution of child pornography [51]. Dark Web users can access thousands of websites and forums dedicated to the sharing of illegal images and videos of children [39]. These images and videos are often obtained through the abuse of children, and the victims are often exploited repeatedly over a long period.

Another form of child exploitation on the Dark Web is the live streaming of child sexual abuse [76]. This involves the live streaming of a child being sexually abused or assaulted. Perpetrators can pay for access to these streams, and some even request specific acts or scenarios to be carried out on camera [76].

In addition to these forms of exploitation, the Dark Web is also used for the trafficking of children [77]. Criminals can use the Dark Web to find potential victims, arrange meetings, and make payments. This allows them to operate with a degree of anonymity and avoid detection by law enforcement agencies.

Child exploitation on the Dark Web poses a significant danger to children. It can lead to long-term physical and psychological damage, including depression, anxiety, and post-traumatic stress disorder [56]. The children involved are often subject to ongoing abuse, and their images can be shared online indefinitely, perpetuating the trauma they have experienced.

It is difficult to provide accurate statistics on child exploitation on the Dark Web as it is an underground and illegal activity that is difficult to track. However, here are some statistics related to child exploitation on the Dark Web in 2021:

- In the study 'Protecting Children's Rights: A Comparative Analysis between Vietnam and the Legal Models of the European Union and Hungary' [78], it was revealed that over 2200 individuals were identified in cases related to child abuse, underscoring the pervasive issue of child exploitation within these regions.
- The research 'Online Child Sexual Exploitation and Abuse: Criminal Justice Pathways of Police-Reported Incidents in Canada, 2014 to 2020' [79] highlights the critical issue of online child exploitation in Canada, detailing the pathways through the criminal justice system for such cases over a six-year period.
- An anthropological investigation titled 'An Anthropological Investigation of Assam—the Human Trafficking Hub of India?' [80] examines Assam's significant challenges with human trafficking and exploitation, particularly affecting vulnerable local children and women.
- A correlational study aimed at analyzing the knowledge and attitude towards early marriage among parents in selected rural areas of Kolhapur District [81] identifies child marriage as a critical form of exploitation, highlighting the need for increased awareness and education among parents to protect children's rights.

These statistics highlight the disturbing and increasing trend of child exploitation on the Dark Web and the need for continued efforts to combat this issue. It is important to note that these statistics likely represent only a fraction of the actual instances of child exploitation on the Dark Web, as many cases go unreported or undetected.

4.1.5. Money Laundering

Money laundering on the Dark Web takes many forms. One common method is the use of cryptocurrency to launder money [82]. Criminals can use the anonymity provided by cryptocurrency transactions to transfer money without detection [26]. They can also use mixers and tumblers to obscure the origin of the funds and make it more difficult to trace the transactions. Another method of money laundering on the Dark Web is through the use of virtual currencies. Criminals can use these currencies to buy and sell goods and services on Dark Web marketplaces, such as drugs and weapons, and then convert the virtual currency into cash [83]. In addition to these methods, the Dark Web is also used for traditional money laundering techniques, such as smurfing and structuring. Smurfing involves breaking up large amounts of money into smaller, more manageable amounts,

and structuring involves making deposits or withdrawals in a way that avoids detection by financial institutions [41]. Money laundering on the Dark Web poses a significant danger to society [54]. It allows criminals to profit from illegal activities, such as drug trafficking and human trafficking, and use the profits to fund further criminal enterprises. This can lead to an increase in organized crime, violence, and corruption, which can undermine the rule of law and threaten the stability of society [84].

Efforts are being made to combat money laundering on the Dark Web. Law enforcement agencies around the world are working together to identify and prosecute those involved in money laundering, and many have had success in shutting down Dark Web marketplaces that facilitate money laundering [38].

In addition to law enforcement efforts, there are also several initiatives being led by governments and international organizations to combat money laundering on the Dark Web. For example, the Financial Action Task Force (FATF), an intergovernmental organization focused on combating money laundering and terrorism financing, has issued guidance on virtual currencies and the risks they pose to the global financial system [85].

Technology companies are also taking steps to combat money laundering on the Dark Web [27]. Many have developed tools to identify and track cryptocurrency transactions, and some have even created databases of known money laundering techniques and patterns to help law enforcement agencies identify criminals.

4.1.6. Espionage

Espionage on the Dark Web takes many forms. One common method is the use of anonymous communication channels, such as encrypted messaging apps, to exchange sensitive information between agents [45]. These communications can be encrypted end-to-end, making it virtually impossible for law enforcement and intelligence agencies to intercept and decipher the messages. Another method of espionage on the Dark Web is through the use of fake social media accounts and websites. Agents can use these accounts and websites to spread propaganda, collect information about their targets, and recruit new agents [28]. The anonymity provided by the Dark Web makes it difficult for intelligence agencies to track down the individuals behind these accounts and websites.

In addition to these methods, the Dark Web is also used for cyber espionage [86]. Cyber espionage involves using hacking and other cyber-attacks to gain access to sensitive information, such as classified government documents and military secrets. The Dark Web provides a platform for cybercriminals and nation-state actors to buy and sell hacking tools, exploit kits, and other cyber weapons [47].

Espionage on the Dark Web poses a significant danger to national security. It allows foreign governments and criminal organizations to collect sensitive information about a country's military, economic, and political activities, which can be used to undermine its security and stability [87]. It can also lead to the theft of intellectual property and trade secrets, which can have significant economic implications. Efforts are being made to combat espionage on the Dark Web. Intelligence agencies around the world are working together to identify and prosecute those involved in espionage activities, and many have had success in shutting down Dark Web marketplaces that facilitate espionage activities [88].

In addition to law enforcement efforts, there are also several initiatives being led by governments and international organizations to combat espionage on the Dark Web. For example, the Five Eyes intelligence alliance, which includes the United States, United Kingdom, Canada, Australia, and New Zealand, has established a joint cyber threat intelligence sharing platform to share information about cyber threats and espionage activities [89].

Unfortunately, there are no specific statistics on espionage on the Dark Web as it is a covert activity and is not easily tracked or measured. However, there have been several high-profile cases of espionage and cyber-attacks attributed to state-sponsored actors using the Dark Web as a platform for their activities.

- The WannaCry attack in 2017 not only disrupted IT systems but also had tangible effects on healthcare services, particularly within the UK's National Health Service

(NHS). A study analyzing the impact of WannaCry on the NHS found a notable decrease in hospital activity, including a 6% drop in total admissions per day during the attack. Emergency admissions decreased by 4% and elective admissions by 9%, and there were significantly fewer A&E attendances and outpatient services. The economic value of reduced activity in infected trusts during the attack week was estimated at GBP 5.9 million. If all trusts had been affected similarly, the total value of lost activity could have amounted to GBP 35 million [90].

- In another case, in 2018, the United States Department of Justice indicted 12 Russian intelligence officers for their involvement in hacking the Democratic National Committee during the 2016 US presidential election. The hackers used the Dark Web to communicate and exchange stolen information, and they were able to evade detection for several years [91].

These examples highlight the serious threat that espionage on the Dark Web poses to national security and the global economy. While specific statistics are difficult to come by, espionage on the Dark Web is a growing concern for governments and intelligence agencies around the world.

4.2. Tracking the Criminals on the Dark Web

Tracking criminals on the Dark Web is a challenging task, as it is designed to be an anonymous and untraceable environment [92]. However, there are several techniques and tools that can be used to track down criminals and their illegal activities on the Dark Web [36]. Here are some of the techniques commonly used:

1. **Data Mining**: This involves using advanced data analysis tools to collect and analyze large volumes of data from various sources on the Dark Web, such as online marketplaces, forums, and social media platforms [43]. The data can include keywords, images, and metadata, which can be used to identify patterns and links between criminal activities and the individuals involved.
2. **Blockchain Analysis**: Many illegal transactions on the Dark Web are conducted using cryptocurrencies like Bitcoin, which offer a high degree of anonymity [50]. However, all transactions on the blockchain are publicly recorded, and this data can be used to trace the flow of funds and identify individuals involved in criminal activities.
3. **Social Engineering**: This involves using psychological manipulation techniques to trick criminals into revealing their identities or locations [93]. Social engineering tactics can include phishing emails, fake social media accounts, and other types of online impersonation.
4. **Law Enforcement Collaboration**: Law enforcement agencies around the world are increasingly collaborating to share information and resources to locate and arrest criminals on the Dark Web [30]. This includes the use of international arrest warrants, extradition agreements, and joint task forces.
5. **Dark Web Crawlers**: These are automated tools that search the Dark Web for specific keywords or phrases and can help identify illegal activities, marketplaces, and individuals involved in criminal activities. While Deep Web crawling is included under data mining due to its broader focus on non-indexed online content, Dark Web crawling is separately categorized because it specifically targets encrypted and anonymized networks such as TOR. This requires specialized techniques and tools distinct from those used for general data mining, emphasizing the unique challenges and methodologies associated with investigating the Dark Web [24].
6. **Human Intelligence**: While technology can help locate criminals on the Dark Web, it is often human intelligence that provides the most valuable information [17]. This can include tips from informants, undercover agents, and whistleblowers.

Tracking criminals on the Dark Web is a difficult task, but there are several techniques and tools available to law enforcement and intelligence agencies to track down illegal activities and arrest those involved.

4.2.1. Data Mining

Data mining is one of the most powerful techniques for tracking criminals on the Dark Web. It involves collecting and analyzing large volumes of data from various sources on the Dark Web, such as online marketplaces, forums, and social media platforms. While Deep Web crawling is included under data mining due to its broader focus on non-indexed online content, Dark Web crawling is separately categorized because it specifically targets encrypted and anonymized networks such as TOR. This requires specialized techniques and tools distinct from those used for general data mining, emphasizing the unique challenges and methodologies associated with investigating the Dark Web. Here are some ways that data mining can be used to track criminals on the Dark Web:

- Keyword Search: Data mining tools can be used to search for specific keywords or phrases that are associated with criminal activities [24]. These keywords can include terms related to drug trafficking, human trafficking, weapons smuggling, and other illegal activities. By collecting data on these keywords, law enforcement agencies can identify the individuals and groups involved in these activities and take appropriate action.
- Image Recognition: Data mining tools can also be used to recognize and analyze images posted on the Dark Web [20]. For example, images of weapons, drugs, and other illegal items can be identified and used to track down the individuals involved in their sale and distribution.
- Network Analysis: Data mining tools can be used to identify patterns and links between individuals and groups involved in criminal activities on the Dark Web. By analyzing the network of connections between these individuals, law enforcement agencies can identify the most influential players and take targeted action to disrupt their activities [94].
- Sentiment Analysis: Data mining tools can also be used to analyze the sentiment of online discussions related to criminal activities [95]. This can help law enforcement agencies identify potential threats and take proactive measures to prevent them from occurring.
- Deep Web Crawling: Data mining tools can be used to crawl the Deep Web, which includes parts of the Dark Web that are not easily accessible using standard search engines [40]. By collecting data from these hidden areas, law enforcement agencies can gain a more complete understanding of the criminal activities taking place on the Dark Web.

Data mining is a powerful tool for tracking criminals on the Dark Web. By collecting and analyzing large volumes of data from various sources, law enforcement agencies can identify patterns and links between individuals and groups involved in criminal activities and take appropriate action to disrupt their activities. However, it is important to note that data mining is only one part of a larger strategy for combating crime on the Dark Web, and it must be used in combination with other techniques and tools in order for it to be effective.

4.2.2. Blockchain Analysis

Blockchain analysis is another powerful technique that can be used to track criminals on the Dark Web. Blockchain is a decentralized, digital ledger that records transactions in a transparent and immutable manner. Here are some ways that blockchain analysis can be used to track criminals on the Dark Web:

- Address Clustering: Blockchain analysis tools can be used to cluster together different addresses that are owned by the same individual or entity [31]. This can help law enforcement agencies to identify the parties involved in a particular transaction or activity on the blockchain.
- Transaction Tracing: Blockchain analysis tools can also be used to trace the flow of funds on the blockchain. By following the trail of transactions, law enforcement

agencies can identify the source and destination of funds, and the individuals and entities involved in the transaction [44].

- Taint Analysis: Taint analysis is a technique used to identify the origin of tainted funds on the blockchain. Tainted funds are those that have been used for criminal activities, such as drug trafficking or money laundering. By analyzing the transactions involving tainted funds, law enforcement agencies can track down the individuals and entities involved in these activities [96].
- Pattern Recognition: Blockchain analysis tools can be used to identify patterns in the transactions on the blockchain. For example, patterns may emerge in the amounts of funds transferred or in the timing of transactions. By analyzing these patterns, law enforcement agencies can identify potential criminal activity and take appropriate action.
- Blockchain Data Mining: Blockchain data mining involves analyzing the blockchain to identify trends and patterns that may be indicative of criminal activity. This can involve analyzing the metadata associated with transactions, such as the time and location of transactions, as well as the types of transactions taking place [97].

4.2.3. Social Engineering

Social engineering is a technique used to manipulate individuals into divulging sensitive information or performing certain actions. While social engineering is often used by cybercriminals to commit fraud or steal sensitive information, it can also be used by law enforcement agencies to track criminals on the Dark Web. Here are some ways that social engineering can be used to track criminals:

- Phishing Attacks: Phishing attacks are a type of social engineering attack that involves sending fraudulent emails or messages in order to trick individuals into divulging sensitive information. By sending phishing emails or messages to Dark Web users, law enforcement agencies can potentially obtain information about the individuals and groups involved in criminal activities.
- Impersonation: Impersonation is another social engineering technique that can be used to track criminals. Law enforcement agencies may create fake profiles or personas in order to gain the trust of Dark Web users and obtain information about criminal activities.
- Spear Phishing: Spear phishing is a more targeted type of phishing attack that is directed at specific individuals or groups. By sending spear phishing emails or messages to Dark Web users, law enforcement agencies can potentially obtain more detailed information about the individuals and groups involved in criminal activities.
- Vishing: Vishing is a type of social engineering attack that involves using voice communication to trick individuals into divulging sensitive information [98]. Law enforcement agencies may use vishing techniques to obtain information about criminal activities on the Dark Web.
- Reverse Social Engineering: Reverse social engineering is a technique that involves manipulating individuals into taking certain actions, such as clicking on a link or downloading a file, in order to track their activities. Law enforcement agencies may use reverse social engineering techniques to track the activities of Dark Web users.

4.2.4. Law Enforcement Collaboration

Law enforcement collaboration is a crucial tool in tracking criminals on the Dark Web. Due to the nature of the Dark Web, which allows users to remain anonymous and operate without detection, tracking criminals on this platform can be a challenging task [53]. However, with the help of collaboration and information sharing between law enforcement agencies, it is possible to overcome these challenges and successfully track down criminals on the Dark Web. Here are some ways that law enforcement collaboration can be used to track criminals on the Dark Web:

- Information Sharing: Law enforcement agencies can share information and intelligence about criminal activities on the Dark Web. This can include information about criminal

networks, modus operandi, and tactics. By sharing information, law enforcement agencies can build a more complete picture of criminal activities on the Dark Web and identify potential targets for investigation.
- Joint Investigations: Law enforcement agencies can collaborate on joint investigations into criminal activities on the Dark Web. By combining their resources and expertise, law enforcement agencies can conduct more effective investigations and improve their chances of tracking down criminals.
- International Cooperation: Many criminal activities on the Dark Web are international in scope. Law enforcement agencies can work together across international borders to share information and intelligence, conduct joint investigations, and bring criminals to justice.
- Cross-Agency Training: Law enforcement agencies can provide training and support to one another on how to investigate and track criminals on the Dark Web. This can include training on technical tools and techniques, as well as sharing best practices for investigating and prosecuting cybercrime.
- Task Forces: Law enforcement agencies can form task forces to focus on specific types of criminal activities on the Dark Web. For example, task forces can be established to investigate child exploitation, drug trafficking, or money laundering on the Dark Web. By pooling their resources and expertise, task forces can conduct more targeted and effective investigations.

4.2.5. Dark Web Crawlers

Dark Web crawlers, also known as web scrapers, can be used to collect and analyze data from the Dark Web. These tools can be used by law enforcement agencies to track criminals and gather information about criminal activities on the Dark Web [18]. Here are some ways that Dark Web crawlers can be used to track criminals:

- Data Collection: Dark Web crawlers can be used to collect data from the Dark Web, including information about criminal activities, criminal networks, and potential targets for investigation. Crawlers can be configured to scrape specific websites, forums, and chat rooms for information, and the data collected can be used to build a more complete picture of criminal activities on the Dark Web.
- Analysis: Once data have been collected, Dark Web crawlers can be used to analyze the data and identify patterns and trends. This analysis can help law enforcement agencies to identify potential targets for investigation and to build a case against individuals involved in criminal activities on the Dark Web.
- Threat Intelligence: Dark Web crawlers can also be used to gather threat intelligence, including information about emerging threats and vulnerabilities on the Dark Web. This information can be used to inform law enforcement strategies and to develop new tools and techniques for investigating criminal activities on the Dark Web.
- Automated Alerts: Dark Web crawlers can be configured to provide automated alerts when certain keywords or topics are detected. For example, a crawler could be configured to send an alert when it detects mentions of a specific criminal network or the sale of a particular illegal item on the Dark Web. These alerts can help law enforcement agencies to respond quickly to emerging threats and to gather intelligence about criminal activities.

Overall, Dark Web crawlers can be a powerful tool for law enforcement agencies to track criminals and gather intelligence about criminal activities on the Dark Web. However, it is important to note that the use of Dark Web crawlers must be carried out in accordance with the law and with appropriate privacy protections for the individuals involved in investigations.

4.2.6. Human Intelligence

Human intelligence (HUMINT) is a key component of tracking criminals on the Dark Web. HUMINT involves gathering information from human sources, such as informants or

undercover agents, rather than relying solely on technical tools and analysis [99]. Here are some ways that HUMINT can be used to track criminals on the Dark Web:

- Undercover Operations: Law enforcement agencies can use undercover agents to infiltrate criminal networks on the Dark Web. These agents can gather intelligence on criminal activities and help to identify key players in the network. Undercover operations can be risky, but they can provide valuable information that would be difficult to obtain through other means.
- Informants: Informants are individuals who provide information to law enforcement agencies in exchange for some form of benefit or protection. Informants can be particularly valuable on the Dark Web, where anonymity is a key factor. By providing information about criminal activities, informants can help law enforcement agencies to identify targets for investigation and build a case against individuals involved in criminal activities on the Dark Web.
- Community Outreach: Law enforcement agencies can also engage with communities that are vulnerable to exploitation on the Dark Web, such as victims of online child sexual exploitation. By building trust with these communities, law enforcement agencies can gather valuable information about criminal activities on the Dark Web and provide support to victims.
- Collaboration: Collaboration between law enforcement agencies can also be a valuable source of HUMINT. By sharing information and resources, agencies can work together to identify and track criminals on the Dark Web. Collaboration can also help to build a more complete picture of criminal activities on the Dark Web, making it easier to identify and disrupt criminal networks.

Overall, HUMINT is a critical component of tracking criminals on the Dark Web. By combining technical tools and analysis with human intelligence, law enforcement agencies can build a comprehensive understanding of criminal activities on the Dark Web and take action to disrupt these activities. However, it is important to note that the use of HUMINT must be carried out in accordance with the law and with appropriate privacy protections for the individuals involved in investigations.

4.3. Summative Evaluation of the Studies

Cybercrime is perhaps the most significant emerging crime threat on the Dark Web. This includes activities such as hacking, phishing, identity theft, and malware distribution. The anonymity provided by the Dark Web makes it easier for cybercriminals to operate without fear of being caught, and cryptocurrencies are often used to facilitate illegal transactions.

Drug trafficking is another emerging crime threat on the Dark Web. The anonymity of the Dark Web has made it easier for drug dealers to sell their products without being detected by law enforcement. Buyers can purchase drugs anonymously using cryptocurrencies, and the drugs are often shipped directly to the buyer's address, making it difficult for law enforcement to intercept.

Human trafficking is also a growing concern on the Dark Web. Criminals use the anonymity provided by the Dark Web to recruit, sell, and transport victims of human trafficking. The victims are often forced into labor or prostitution and are subjected to violence and exploitation.

Furthermore, money laundering is another significant emerging crime threat on the Dark Web. Criminals use the Dark Web to launder money obtained through illegal activities, such as drug trafficking and cybercrime. They use cryptocurrencies to hide the origin and destination of the funds, making it difficult for law enforcement to track and trace the money.

The anonymity provided by the Dark Web makes it challenging to identify and prosecute perpetrators of crimes. However, law enforcement agencies have developed several methods to identify and track criminals on the Dark Web.

One method used to identify perpetrators of crimes on the Dark Web is through the use of advanced technology such as artificial intelligence and machine learning. These technologies can help law enforcement agencies sift through large amounts of data to identify patterns and connections between criminal activities and individuals.

Another method used by law enforcement agencies is through the use of undercover operatives. These operatives infiltrate illegal marketplaces and forums on the Dark Web to gather information and build cases against criminals. The use of undercover operatives can be risky, but it has proven to be an effective way to gather intelligence on criminal activities.

Additionally, law enforcement agencies often work in collaboration with international partners to track down criminals on the Dark Web. This cooperation involves the sharing of information and resources, which can help to identify and track down criminals across borders.

Furthermore, law enforcement agencies also use traditional investigative techniques such as surveillance, wiretapping, and physical surveillance to track down perpetrators of crimes on the Dark Web. These methods are often used in conjunction with advanced technology and undercover operatives to build strong cases against criminals.

5. Discussion

The findings from our study highlight several critical aspects of the weaponization of cybercrimes within the Dark Net, offering valuable insights into the current landscape and its implications. The primary emerging threats identified include cybercrime-as-a-service, illegal marketplaces, identity theft, child exploitation, money laundering, and espionage. Each of these activities leverages the anonymity and encryption provided by the Dark Net to operate with impunity, presenting significant challenges to law enforcement and cybersecurity professionals.

One of the most concerning aspects is the rise of Cybercrime-as-a-Service (CaaS), which democratizes cybercriminal activities by making sophisticated tools and services accessible to individuals with limited technical expertise. This model has significantly lowered the barrier to entry for cybercriminal activities, leading to an increase in the frequency and severity of cyber-attacks. The implications of this trend are profound, as it not only escalates the volume of attacks but also diversifies the range of threats, making it more challenging for defenders to anticipate and mitigate them effectively.

Illegal marketplaces on the Dark Net facilitate the trade of a wide array of illicit goods and services, from drugs and weapons to stolen data and hacking tools. These marketplaces operate with sophisticated security measures to evade detection, complicating efforts to dismantle them. The persistence and evolution of these marketplaces underscore the need for continuous advancements in detection and tracking technologies, as well as international cooperation to address the cross-border nature of these crimes.

Identity theft remains a lucrative business on the Dark Net, with personal information being bought and sold regularly. The availability of this data fuels various forms of fraud and financial crimes, with long-lasting impacts on victims' financial health and privacy. Enhanced measures for protecting personal data and more robust mechanisms for detecting and responding to data breaches are crucial to mitigate this threat.

Child exploitation on the Dark Net is particularly egregious, involving the distribution of child pornography, live streaming of abuse, and trafficking. The implications for victims are severe, leading to lasting psychological and physical harm. Tackling this issue requires not only advanced technological solutions but also strong international legal frameworks and dedicated resources for victim support and rehabilitation.

Money laundering on the Dark Net, often facilitated through cryptocurrencies, poses a significant threat to financial systems globally. The anonymous nature of these transactions makes it difficult to trace and prosecute offenders. Strengthening regulatory frameworks around cryptocurrency transactions and developing advanced analytics for detecting suspicious activities are essential steps in combating this form of crime.

Espionage activities on the Dark Net, involving the exchange of sensitive information and cyber-attacks on critical infrastructure, highlight the strategic use of this platform by state and non-state actors. The implications for national security are significant, necessitating a coordinated response that includes improved cyber defense mechanisms and international cooperation to monitor and counter these threats effectively.

In conclusion, the weaponization of cybercrimes on the Dark Net presents a multifaceted threat landscape that requires a comprehensive and coordinated approach to address. This includes advancing technological solutions for detection and prevention, strengthening international legal and regulatory frameworks, and enhancing collaboration among law enforcement agencies worldwide. The findings of our study provide a foundation for understanding these challenges and developing strategies to mitigate their impact, ultimately contributing to a safer and more secure digital environment.

6. Limitations and Threats to Validity

While our study provides valuable insights into the weaponization of cybercrimes on the Dark Net, it is not without limitations. One significant limitation is the reliance on publicly available data, which may not capture the full scope of activities on the Dark Net. This data is often incomplete or biased, as much of the Dark Net's content is hidden or encrypted, making it difficult to obtain a comprehensive view. Additionally, our study primarily uses data from 2011 to 2023, including available studies in 2024, which may not reflect the most current trends and developments in cybercrime.

Another limitation is the potential for selection bias in the articles and sources reviewed. Our systematic literature review included 88 articles, but the selection process might have inadvertently excluded relevant studies that could provide additional insights. This selection bias can affect the generalizability of our findings, as the chosen articles may not represent the entire body of research on Dark Net cybercrimes. Future studies should aim to include a broader range of sources to mitigate this bias.

The rapidly evolving nature of cybercrime presents another threat to the validity of our findings. Cybercriminals continuously adapt their tactics and tools to evade detection and law enforcement efforts, which means that the methods and trends identified in our study may quickly become outdated. To maintain the relevance and accuracy of research in this field, continuous monitoring and updating of data are necessary. Researchers should remain vigilant and adapt their methodologies to capture new developments in cybercrime.

Lastly, the ethical and legal considerations surrounding research on the Dark Net pose challenges to the validity of our study. Accessing and analyzing Dark Net content can raise ethical issues, as it involves engaging with potentially harmful and illegal material. Additionally, legal restrictions on accessing and using Dark Net data can limit the scope of research. Researchers must navigate these ethical and legal challenges carefully to ensure that their work adheres to ethical guidelines and legal requirements while still providing valuable insights into Dark Net activities.

7. Economic and Ethical Impacts

The economic impacts of cybercrimes on the Dark Web are substantial and far-reaching. Cybercrimes such as fraud, identity theft, and ransomware attacks result in significant financial losses for individuals, businesses, and governments. For instance, ransomware attacks can lead to substantial ransom payments, while identity theft can drain personal and corporate accounts. Organizations must also invest heavily in cybersecurity measures to prevent, detect, and respond to cybercrimes. This includes costs associated with hiring cybersecurity professionals, purchasing security software, and conducting regular security audits. Moreover, the broader economic consequences of cybercrimes include reduced consumer confidence in online transactions, disruptions to business operations, and impacts on national economies. Cyber-attacks on critical infrastructure, such as financial systems or healthcare services, can have cascading effects on the economy, further illustrating the extensive economic ramifications of cybercrime activities on the Dark Web.

The ethical implications of cybercrimes on the Dark Web are profound, touching on issues of privacy, consent, and the moral responsibilities of various stakeholders. Cybercrimes often involve significant breaches of privacy, with personal data being stolen, sold, or misused without consent. This raises ethical concerns about the right to privacy and the responsibilities of organizations to protect sensitive information. Additionally, activities such as human trafficking, child exploitation, and illegal drug sales facilitated by the Dark Web have severe ethical implications. They involve the exploitation and harm of vulnerable individuals, raising questions about societal responsibilities to protect these individuals and prevent such crimes. There are also ethical questions regarding the responsibilities of various stakeholders, including governments, businesses, and individuals, in combating cybercrimes. This includes debates on the balance between surveillance for security purposes and the protection of civil liberties, as well as the ethical use of cybersecurity tools. These ethical considerations underscore the complex moral landscape surrounding the battle against cybercrimes on the Dark Web.

8. Conclusions and Future Research Directions

8.1. Conclusions

This study provided a detailed examination of the weaponization of cybercrimes within the Dark Net, using a Systematic Literature Review (SLR) to explore the evolution of cybercrime tactics, their impacts, and the ongoing efforts in detection and mitigation. We synthesized findings from 88 pertinent articles, extending our discussion to cover the implications of these cybercrimes on social, economic, and ethical fronts.

Our investigation highlighted how cybercriminals exploit the anonymous and encrypted nature of the Dark Net to perpetuate crimes ranging from identity theft to sophisticated ransomware attacks. The key challenges identified include the difficulty in tracking and tracing such activities due to the inherent anonymization techniques employed within the Dark Net infrastructure.

8.2. Future Research Directions

Based on the findings and the gaps identified in the literature, we propose several key areas for future research:

8.2.1. Development of Advanced Detection Technologies

Future research should prioritize the development of cutting-edge detection technologies that can adapt to the dynamic nature of the Dark Net. This includes the creation of adaptive AI systems that can predict and respond to cyber threats in real-time, providing a proactive rather than reactive defense mechanism.

8.2.2. Enhancement of Blockchain Analytics

With the rise of cryptocurrency use on the Dark Net, enhancing blockchain analytics will be crucial for tracing illicit transactions. Future studies should focus on the integration of blockchain with artificial intelligence to develop more sophisticated tracking tools that can uncover the financial networks behind cybercrimes.

8.2.3. Strengthening International Collaboration

Cybercrimes on the Dark Net are a global issue that requires a coordinated international response. Future research should explore effective strategies for enhancing collaboration between countries, including shared databases and joint task forces, to combat cybercrimes more effectively.

8.2.4. Ethical and Legal Frameworks

As detection technologies become more invasive, the need for robust ethical and legal frameworks becomes paramount. Future research should delve into the development of

international guidelines that balance the need for security with the protection of individual privacy rights.

8.2.5. Socio-Economic Impact Studies

To fully understand the scope of Dark Net cybercrimes, future research should also include studies on their socio-economic impacts. This includes the effects on individual victims, businesses, and the broader economic implications of widespread cyber insecurity.

8.2.6. Policy and Technological Innovation

Lastly, there is a pressing need for continuous innovation in policies and technologies to keep pace with the fast-evolving cybercrime techniques. Future research could explore the development of new legislative frameworks, as well as the potential for emerging technologies like quantum computing and its implications for cybersecurity.

8.3. Final Thoughts

In conclusion, this paper calls for a sustained and dynamic approach to researching Dark Net cybercrimes. By addressing these future research directions, we can hope to stay ahead of cybercriminals and safeguard our digital futures. As the threat landscape evolves, so must our strategies and tools to combat these digital threats effectively.

Author Contributions: Conceptualization, A.A. and M.N.; methodology, A.A.; validation, A.A. and M.N.; formal analysis, A.A.; investigation, A.A.; resources, M.N.; data curation, M.N.; writing—original draft preparation, A.A.; writing—review and editing, M.N.; visualization, A.A.; supervision, A.A.; project administration, A.A.; funding acquisition, M.N. All authors have read and agreed to the published version of the manuscript.

Funding: The article processing charge was funded by New Zealand Skills and Education College.

Data Availability Statement: The authors confirm that all data generated or analyzed during this study are included in this published article.

Conflicts of Interest: The authors declare no competing interests.

References

1. Lawrence, S.; Giles, C.L. Searching the World Wide Web. *Science* **1998**, *280*, 98–100. [CrossRef] [PubMed]
2. Kaur, S.; Randhawa, S. Dark Web: A Web of Crimes. *Wirel. Pers. Commun.* **2020**, *112*, 2131–2158. [CrossRef]
3. Al Nabki, M.W.; Fidalgo, E.; Alegre, E.; de Paz, I. Classifying Illegal Activities on Tor Network Based on Web Textual Contents. In *Long Papers, Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics, Valencia, Spain, 3–7 April 2017*; Association for Computational Linguistics: Valencia, Spain, 2017; Volume 1, pp. 35–43. Available online: https://aclanthology.org/E17-1004 (accessed on 17 March 2023).
4. Sharma, S.; Sharma, P. Dark Web and Trading of Illegal Drugs. *J. Forensic Sci. Crim. Investig.* **2018**, *9*, 555766.
5. Davis, S.; Arrigo, B. The Dark Web and anonymizing technologies: Legal pitfalls, ethical prospects, and policy directions from radical criminology. *Crime Law Soc. Chang.* **2021**, *76*, 367–386. [CrossRef]
6. Kavallieros, D.; Myttas, D.; Kermitsis, E.; Lissaris, E.; Giataganas, G.; Darra, E. Understanding the Dark Web. In *Dark Web Investigation*; Akhgar, B., Gercke, M., Vrochidis, S., Gibson, H., Eds.; Security Informatics and Law Enforcement; Springer International Publishing: Cham, Switzerland, 2021; pp. 3–26. [CrossRef]
7. Montieri, A.; Ciuonzo, D.; Aceto, G.; Pescapé, A. Anonymity Services Tor, I2P, JonDonym: Classifying in the Dark. In Proceedings of the 2017 29th International Teletraffic Congress (ITC 29), Genoa, Italy, 4–8 September 2017; Volume 1, pp. 81–89. [CrossRef]
8. Dredge, S. What Is Tor? A Beginner's Guide to the Privacy Tool. The Guardian. 5 November 2013. Available online: https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser (accessed on 3 March 2024).
9. Tan, Q.; Wang, X.; Shi, W.; Tang, J.; Tian, Z. An Anonymity Vulnerability in Tor. *IEEE/ACM Trans. Netw.* **2022**, *30*, 2574–2587. [CrossRef]
10. Luong, H.T. Foundations and trends in the darknet-related criminals in the last 10 years: A systematic literature review and bibliometric analysis. *Secur. J.* **2023**. [CrossRef]
11. Ruiz Ródenas, J.M.; Pastor-Galindo, J.; Gómez Mármol, F. A general and modular framework for dark web analysis. *Cluster Comput.* **2023**. [CrossRef]
12. Sarkar, G.; Shukla, S.K. Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *J. Econ. Criminol.* **2023**, *2*, 100034. [CrossRef]

13. Mengist, W.; Soromessa, T.; Legese, G. Method for conducting systematic literature review and meta-analysis for environmental science research. *MethodsX* **2020**, *7*, 100777. [CrossRef]
14. Kitchenham, B.; Charters, S. Guidelines for performing Systematic Literature Reviews in Software Engineering; 2007; Volume 2. Available online: https://www.scirp.org/reference/ReferencesPapers?ReferenceID=1555797 (accessed on 21 May 2024).
15. Chen, H. Dark Web: Exploring and Mining the Dark Side of the Web. In Proceedings of the 2011 European Intelligence and Security Informatics Conference, Athens, Greece, 12–14 September 2011; pp. 1–2. [CrossRef]
16. Bahamazava, K.; Nanda, R. The shift of DarkNet illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence. *Forensic Sci. Int. Digit. Investig.* **2022**, *40*, 301377. [CrossRef]
17. Basheer, R.; Alkhatib, B. Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. *J. Comput. Netw. Commun.* **2021**, *2021*, e1302999. [CrossRef]
18. Bergman, J.; Popov, O.B. Exploring Dark Web Crawlers: A Systematic Literature Review of Dark Web Crawlers and Their Implementation. *IEEE Access* **2023**, *11*, 35914–35933. [CrossRef]
19. Bermudez Villalva, D.A.; Onaolapo, J.; Stringhini, G.; Musolesi, M. Under and over the surface: A comparison of the use of leaked account credentials in the Dark and Surface Web. *Crime Sci.* **2018**, *7*, 17. [CrossRef]
20. Biswas, R.; Fidalgo, E.; Alegre, E. Recognition of service domains on TOR dark net using perceptual hashing and image classification techniques. In Proceedings of the 8th International Conference on Imaging for Crime Detection and Prevention (ICDP 2017), Madrid, Spain, 13–15 December 2017; pp. 7–12. [CrossRef]
21. Cherqi, O.; Mezzour, G.; Ghogho, M.; El Koutbi, M. Analysis of Hacking Related Trade in the Darkweb. In Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA, 8–10 November 2018; pp. 79–84. [CrossRef]
22. Chertoff, M. A public policy perspective of the Dark Web. *J. Cyber Policy* **2017**, *2*, 26–38. [CrossRef]
23. Dalins, J.; Wilson, C.; Carman, M. Criminal motivation on the dark web: A categorisation model for law enforcement. *Digit. Investig.* **2018**, *24*, 62–71. [CrossRef]
24. Dalvi, A.; Paranjpe, S.; Amale, R.; Kurumkar, S.; Kazi, F.; Bhirud, S.G. SpyDark: Surface and Dark Web Crawler. In Proceedings of the 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India, 21–23 May 2021; pp. 45–49. [CrossRef]
25. ElBahrawy, A.; Alessandretti, L.; Rusnac, L.; Goldsmith, D.; Teytelboym, A.; Baronchelli, A. Collective dynamics of dark web marketplaces. *Sci. Rep.* **2020**, *10*, 18827. [CrossRef] [PubMed]
26. Faccia, A.; Moşteanu, N.R.; Cavaliere, L.P.L.; Mataruna-Dos-Santos, L.J. Electronic Money Laundering, The Dark Side of Fintech: An Overview of the Most Recent Cases. In Proceedings of the 2020 12th International Conference on Information Management and Engineering, Amsterdam, The Netherlands, 16–18 September 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 29–34. [CrossRef]
27. Fronzetti Colladon, A.; Remondi, E. Using social network analysis to prevent money laundering. *Expert Syst. Appl.* **2017**, *67*, 49–58. [CrossRef]
28. Gehl, R.W. Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media Soc.* **2016**, *18*, 1219–1235. [CrossRef]
29. Georgoulias, D.; Pedersen, J.M.; Falch, M.; Vasilomanolakis, E. A qualitative mapping of Darkweb marketplaces. In Proceedings of the 2021 APWG Symposium on Electronic Crime Research (eCrime), Boston, MA, USA, 1–3 December 2021; pp. 1–15. [CrossRef]
30. Ghappour, A. Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web. *Stan. L. Rev.* **2017**, *69*, 1075. Available online: https://heinonline.org/HOL/Page?handle=hein.journals/stflr69&id=1101&div=&collection= (accessed on 2 March 2024). [CrossRef]
31. Ghosh, S.; Das, A.; Porras, P.; Yegneswaran, V.; Gehani, A. Automated Categorization of Onion Sites for Analyzing the Darkweb Ecosystem. In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Halifax, NS, Canada, 13–17 August 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 1793–1802. [CrossRef]
32. Godawatte, K.; Raza, M.; Murtaza, M.; Saeed, A. Dark Web Along With The Dark Web Marketing And Surveillance. In Proceedings of the 2019 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), Gold Coast, Australia, 5–7 December 2019; pp. 483–485. [CrossRef]
33. Harviainen, J.T.; Haasio, A.; Hämäläinen, L. Drug traders on a local dark web marketplace. In Proceedings of the 23rd International Conference on Academic Mindtrek, Tampere, Finland, 29–30 January 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 20–26. [CrossRef]
34. Hayes, D.R.; Cappa, F.; Cardon, J. A Framework for More Effective Dark Web Marketplace Investigations. *Information* **2018**, *9*, 186. [CrossRef]
35. Hiramoto, N.; Tsuchiya, Y. Measuring dark web marketplaces via Bitcoin transactions: From birth to independence. *Forensic Sci. Int. Digit. Investig.* **2020**, *35*, 301086. [CrossRef]
36. Jacka, K. Beyond the Surface Web: How Criminals Are Utilising the Internet to Commit Crimes. In *Digital Transformation in Policing: The Promise, Perils and Solutions*; Montasari, R., Carpenter, V., Masys, A.J., Eds.; Advanced Sciences and Technologies for Security Applications; Springer International Publishing: Cham, Switzerland, 2023; pp. 109–118. [CrossRef]

37. Kadoguchi, M.; Hayashi, S.; Hashimoto, M.; Otsuka, A. Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning. In Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 1–3 July 2019; pp. 200–202. [CrossRef]
38. Kermitsis, E.; Kavallieros, D.; Myttas, D.; Lissaris, E.; Giataganas, G. Dark Web Markets. In *Dark Web Investigation*; Akhgar, B., Gercke, M., Vrochidis, S., Gibson, H., Eds.; Security Informatics and Law Enforcement; Springer International Publishing: Cham, Switzerland, 2021; pp. 85–118. [CrossRef]
39. Kloess, J.A.; van der Bruggen, M. Trust and Relationship Development Among Users in Dark Web Child Sexual Exploitation and Abuse Networks: A Literature Review From a Psychological and Criminological Perspective. *Trauma Violence Abus.* **2023**, *24*, 1220–1237. [CrossRef] [PubMed]
40. Koloveas, P.; Chantzios, T.; Tryfonopoulos, C.; Skiadopoulos, S. A Crawler Architecture for Harvesting the Clear, Social, and Dark Web for IoT-Related Cyber-Threat Intelligence. In Proceedings of the 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 8–13 July 2019; Volume 2642-939X, pp. 3–8. [CrossRef]
41. Kruisbergen, E.W.; Leukfeldt, E.R.; Kleemans, E.R.; Roks, R.A. Money talks money laundering choices of organized crime offenders in a digital age. *J. Crime Justice* **2019**, *42*, 569–581. [CrossRef]
42. Leonidou, P.; Salamanos, N.; Farao, A.; Aspri, M.; Sirivianos, M. A Qualitative Analysis of Illicit Arms Trafficking on Darknet Marketplaces. In Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy, 29 August–1 September 2023; Association for Computing Machinery: New York, NY, USA, 2023; pp. 1–9. [CrossRef]
43. Marin, E.; Shakarian, J.; Shakarian, P. Mining Key-Hackers on Darkweb Forums. In Proceedings of the 2018 1st International Conference on Data Intelligence and Security (ICDIS), South Padre Island, TX, USA, 8–10 April 2018; pp. 73–80. [CrossRef]
44. Raman, R.; Kumar Nair, V.; Nedungadi, P.; Ray, I.; Achuthan, K. Darkweb research: Past, present, and future trends and mapping to sustainable development goals. *Heliyon* **2023**, *9*, e22269. [CrossRef]
45. Rawat, R.; Mahor, V.; Chirgaiya, S.; Garg, B. Artificial Cyber Espionage Based Protection of Technological Enabled Automated Cities Infrastructure by Dark Web Cyber Offender. In *Intelligence of Things: AI-IoT Based Critical-Applications and Innovations*; Al-Turjman, F., Nayyar, A., Devi, A., Shukla, P.K., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 167–188. [CrossRef]
46. Rawat, R.; Rajawat, A.S.; Mahor, V.; Shaw, R.N.; Ghosh, A. Dark Web—Onion Hidden Service Discovery and Crawling for Profiling Morphing, Unstructured Crime and Vulnerabilities Prediction. In *Innovations in Electrical and Electronic Engineering*; Mekhilef, S., Favorskaya, M., Pandey, R.K., Shaw, R.N., Eds.; In Lecture Notes in Electrical Engineering; Springer: Singapore, 2021; pp. 717–734. [CrossRef]
47. Staley, B.; Montasari, R. A Survey of Challenges Posed by the Dark Web. In *Artificial Intelligence in Cyber Security: Impact and Implications: Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges*; Montasari, R., Jahankhani, H., Eds.; Advanced Sciences and Technologies for Security Applications; Springer International Publishing: Cham, Switzerland, 2021; pp. 203–213. [CrossRef]
48. Tavabi, N.; Bartley, N.; Abeliuk, A.; Soni, S.; Ferrara, E.; Lerman, K. Characterizing Activity on the Deep and Dark Web. In Proceedings of the Companion Proceedings of The 2019 World Wide Web Conference, San Francisco, CA, USA, 13–17 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 206–213. [CrossRef]
49. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233. [CrossRef]
50. Tsuchiya, Y.; Hiramoto, N. Dark web in the dark: Investigating when transactions take place on cryptomarkets. *Forensic Sci. Int. Digit. Investig.* **2021**, *36*, 301093. [CrossRef]
51. van der Bruggen, M.; Blokland, A. A Crime Script Analysis of Child Sexual Exploitation Material Fora on the Darkweb. *Sex. Abus.* **2021**, *33*, 950–974. [CrossRef]
52. Vyas, P.; Vyas, G.; Chauhan, A.; Rawat, R.; Telang, S.; Gottumukkala, M. Anonymous Trading on the Dark Online Marketplace: An Exploratory Study. In *Using Computational Intelligence for the Dark Web and Illicit Behavior Detection*; IGI Global: Hershey, PA, USA, 2022; pp. 272–289. [CrossRef]
53. Warner, C. Law Enforcement and Digital Policing of the Dark Web: An Assessment of the Technical, Ethical and Legal Issues. In *Applications for Artificial Intelligence and Digital Forensics in National Security*; Montasari, R., Ed.; Advanced Sciences and Technologies for Security Applications; Springer Nature Switzerland: Cham, Switzerland, 2023; pp. 105–115. [CrossRef]
54. Weimann, G. Terrorist Migration to the Dark Web. *Perspect. Terror.* **2016**, *10*, 40–44. Available online: https://www.jstor.org/stable/26297596 (accessed on 5 March 2024).
55. Yannikos, Y.; Schäfer, A.; Steinebach, M. Monitoring Product Sales in Darknet Shops. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–7. [CrossRef]
56. Zulkarnine, A.T.; Frank, R.; Monk, B.; Mitchell, J.; Davies, G. Surfacing collaborated networks in dark web to find illicit and criminal content. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28–30 September 2016; pp. 109–114. [CrossRef]
57. Drug Statistics—Worldometer. Available online: https://www.worldometers.info/drugs/ (accessed on 3 March 2024).
58. United Nations: Office on Drugs and Crime. Drug trafficking. Available online: https://www.unodc.org/unodc/en/drug-trafficking/index.html (accessed on 3 March 2024).

59. Broadhurst, R.; Ball, M.; Trivedi, H. Fentanyl availability on darknet markets. *Trends Issues Crime Crim. Justice* **2020**, *590*, 1–14. [CrossRef]
60. Mirea, M.; Wang, V.; Jung, J. The not so dark side of the darknet: A qualitative study. *Secur. J.* **2019**, *32*, 102–118. [CrossRef]
61. Office of Public Affairs, United States Department of Justice. AlphaBay, the Largest Online "Dark Market", Shut Down. Available online: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down (accessed on 3 March 2024).
62. Broséus, J.; Rhumorbarbe, D.; Mireault, C.; Ouellette, V.; Crispino, F.; Décary-Hétu, D. Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Sci. Int.* **2016**, *264*, 7–14. [CrossRef] [PubMed]
63. Manky, D. Cybercrime as a service: A very modern business. *Comput. Fraud. Secur.* **2013**, *2013*, 9–13. [CrossRef]
64. Singh, J.; Rahman, N.A. Cybercrime-As-A-Service (Malware). In Proceedings of the 2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT), Bangalore, India, 20–21 October 2023; pp. 1–5. [CrossRef]
65. Hyslip, T.S. Cybercrime-as-a-Service Operations. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Holt, T.J., Bossler, A.M., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 815–846. [CrossRef]
66. Hyslip, T.S.; Holt, T.J. Assessing the Capacity of DRDoS-For-Hire Services in Cybercrime Markets. *Deviant Behav.* **2019**, *40*, 1609–1625. [CrossRef]
67. Santanna, J.J.; van Rijswijk-Deij, R.; Hofstede, R.; Sperotto, A.; Wierbosch, M.; Granville, L.Z.; Pras, A. Booters—An analysis of DDoS-as-a-service attacks. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 11–15 May 2015; pp. 243–251. [CrossRef]
68. Alwashali, A.A.M.A.; Rahman, N.A.A.; Ismail, N. A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack. In Proceedings of the 2021 14th International Conference on Developments in eSystems Engineering (DeSE), Sharjah, United Arab Emirates, 7–10 December 2021; pp. 92–96. [CrossRef]
69. Ben-Asher, N.; Gonzalez, C. Effects of cyber security knowledge on attack detection. *Comput. Hum. Behav.* **2015**, *48*, 51–61. [CrossRef]
70. Huang, K.; Siegel, M.; Madnick, S. Systematically Understanding the Cyber Attack Business: A Survey. *ACM Comput. Surv.* **2018**, *51*, 1–36. [CrossRef]
71. Cybercrime-as-a-Service: Tackling a Rapidly Professionalising Industry. Trend Micro. Available online: https://www.trendmicro.com/en_gb/research/22/k/cybercrime-as-a-service-tackling-a-rapidly-professionalising-industry.html (accessed on 4 March 2024).
72. Shelley, L.I. *Dark Commerce: How a New Illicit Economy Is Threatening Our Future*; Princeton University Press: Princeton, NJ, USA, 2018.
73. Hummer, D.; Byrne, J.M. *Handbook on Crime and Technology*; Edward Elgar Publishing: Cheltenham, UK, 2023.
74. Identity Theft Resource Center®'s 2020 Annual Data Breach Report Reveals 19 Percent Decrease in Breaches. Available online: https://www.idtheftcenter.org/post/identity-theft-resource-centers-2020-annual-data-breach-report-reveals-19-percent-decrease-in-breaches/ (accessed on 4 March 2024).
75. Sapienza, A.; Bessi, A.; Damodaran, S.; Shakarian, P.; Lerman, K.; Ferrara, E. Early Warnings of Cyber Threats in Online Discussions. In Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW), New Orleans, LA, USA, 18–21 November 2017; pp. 667–674. [CrossRef]
76. Raven, A.; Akhgar, B.; Abdel Samad, Y. Case Studies: Child Sexual Exploitation. In *Dark Web Investigation*; Akhgar, B., Gercke, M., Vrochidis, S., Gibson, H., Eds.; Security Informatics and Law Enforcement; Springer International Publishing: Cham, Switzerland, 2021; pp. 249–266. [CrossRef]
77. Anjum, A.; Kaur, D.C.; Kondapalli, S.; Hussain, M.A.; Begum, A.U.; Hassen, S.M.; Adam Boush, D.M.S.; Benjeed, A.O.S.; Osman Abdalraheem, D.M.H. A Mysterious and Darkside of The Darknet: A Qualitative Study. Rochester, NY, USA, 20 December 2021. Available online: https://papers.ssrn.com/abstract=4167244 (accessed on 4 March 2024).
78. Giang, H.T.T.; Herger, D.E.C. Protecting Children's Rights: A Comparative Analysis between Vietnam and the Legal Models of the European Union and Hungary. Available online: https://md.ajk.pte.hu/sites/default/files/publications/PROTECTING%20CHILDREN'S%20RIGHTS%20.pdf (accessed on 21 May 2024).
79. Ibrahim, D. Online Child Sexual Exploitation and Abuse: Criminal Justice Pathways of Police-Reported Incidents in Canada, 2014 to 2020/by Dyna Ibrahim. 2023. Available online: https://policycommons.net/artifacts/4250149/online-child-sexual-exploitation-and-abuse/5059039/ (accessed on 4 March 2024).
80. Kalita, B.; Sahani, R. An Anthropological Investigation of Assam—The Human Trafficking Hub of India? *Hum. Rights Rev.* **2023**, *24*, 545–566. [CrossRef]
81. Jadhav, T. A Correlational Study to analyze the knowledge and attitude towards early marriage among parents at selected rural areas, Kolhapur District. *A V Pub Int. J. Nurs. Med. Res.* **2023**, *2*, 121–129. [CrossRef]
82. Rebe, N. *Regulating Cyber Technologies: Privacy Vs Security*; World Scientific: London, UK, 2023.
83. van Wegberg, R.; Oerlemans, J.-J.; van Deventer, O. Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *J. Financ. Crime* **2018**, *25*, 419–435. [CrossRef]
84. Wronka, C. "Cyber-laundering": The change of money laundering in the digital age. *J. Money Laund. Control.* **2021**, *25*, 330–344. [CrossRef]

85. Benton, D.; Ryder, N. Terrorism Financing, the United Kingdom, and the Financial Action Task Force: A Series of Omissions or Missed Opportunities? In *Sustainable Finance and Financial Crime*; Dion, M., Ed.; Sustainable Finance; Springer International Publishing: Cham, Switzerland, 2023; pp. 353–374. [CrossRef]
86. Bederna, Z.; Szadeczky, T. Cyber espionage through Botnets. *Secur. J.* **2020**, *33*, 43–62. [CrossRef]
87. Adkins, G. Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism. *J. Strateg. Secur.* **2013**, *6*, 1–9. Available online: https://www.jstor.org/stable/26485051 (accessed on 5 March 2024). [CrossRef]
88. Denker, K.; Schäfer, M.; Steinebach, M. Darknets as Tools for Cyber Warfare. In *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*; Reuter, C., Ed.; Springer Fachmedien: Wiesbaden, Germany, 2019; pp. 107–135. [CrossRef]
89. Lemieux, F.; Lemieux, F. National Security Intelligence in the Five Eyes Countries. In *Intelligence and State Surveillance in Modern Societies*; Emerald Publishing Limited: Leeds, UK, 2018; pp. 33–67. [CrossRef]
90. Ghafur, S.; Kristensen, S.; Honeyford, K.; Martin, G.; Darzi, A.; Aylin, P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *Npj Digit. Med.* **2019**, *2*, 98. [CrossRef] [PubMed]
91. Office of Public Affairs, United States Department of Justice. Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election. Available online: https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election (accessed on 5 March 2024).
92. Horan, C.; Saiedian, H. Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *J. Cybersecur. Priv.* **2021**, *1*, 580–596. [CrossRef]
93. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. [CrossRef]
94. Alharbi, A.; Faizan, M.; Alosaimi, W.; Alyami, H.; Agrawal, A.; Kumar, R.; Khan, R.A. Exploring the Topological Properties of the Tor Dark Web. *IEEE Access* **2021**, *9*, 21746–21758. [CrossRef]
95. Abbasi, A.; Chen, H. Affect Intensity Analysis of Dark Web Forums. In Proceedings of the 2007 IEEE Intelligence and Security Informatics, New Brunswick, NJ, USA, 23–24 May 2007; pp. 282–288. [CrossRef]
96. Tovanich, N.; Cazabet, R. Pattern Analysis of Money Flows in the Bitcoin Blockchain. In *Complex Networks and Their Applications XI*; Cherifi, H., Mantegna, R.N., Rocha, L.M., Cherifi, C., Miccichè, S., Eds.; Studies in Computational Intelligence; Springer International Publishing: Cham, Switzerland, 2023; pp. 443–455. [CrossRef]
97. Faisal, T.; Courtois, N.; Serguieva, A. The Evolution of Embedding Metadata in Blockchain Transactions. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–9. [CrossRef]
98. Alkhalil, Z.; Hewage, C.; Nawaf, L.; Khan, I. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Front. Comput. Sci.* **2021**, *3*, 563060. Available online: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060 (accessed on 5 March 2024). [CrossRef]
99. Unver, A. Digital Open Source Intelligence and International Security: A Primer. Rochester, NY, USA, 15 July 2018. Available online: https://papers.ssrn.com/abstract=3331638 (accessed on 5 March 2024).