Journal of
Cybersecurity and Privacy

MDPI

Systematic Review

SoK: An Evaluation of the Secure End User Experience on the Dark Net through Systematic Literature Review

Faiza Tazi *, Sunny Shrestha, Junibel De La Cruz and Sanchari Das *

InSPIRIT Lab, University of Denver, Denver, CO 80210, USA; sunny.shrestha@du.edu (S.S.);
junibel.delacruz@du.edu (J.D.L.C.)
* Correspondence: faiza.tazi@du.edu (F.T.); sanchari.das@du.edu (S.D.)

Abstract: The World Wide Web (www) consists of the surface web, deep web, and Dark Web, depending on the content shared and the access to these network layers. Dark Web consists of the Dark Net overlay of networks that can be accessed through specific software and authorization schema. Dark Net has become a growing community where users focus on keeping their identities, personal information, and locations secret due to the diverse population base and well-known cyber threats. Furthermore, not much is known of Dark Net from the user perspective, where often there is a misunderstanding of the usage strategies. To understand this further, we conducted a systematic analysis of research relating to Dark Net privacy and security on $N = 200$ academic papers, where we also explored the user side. An evaluation of secure end-user experience on the Dark Net establishes the motives of account initialization in overlaid networks such as Tor. This work delves into the evolution of Dark Net intelligence for improved cybercrime strategies across jurisdictions. The evaluation of the developing network infrastructure of the Dark Net raises meaningful questions on how to resolve the issue of increasing criminal activity on the Dark Web. We further examine the security features afforded to users, motives, and anonymity revocation. We also evaluate more closely nine user-study-focused papers revealing the importance of conducting more research in this area. Our detailed systematic review of Dark Net security clearly shows the apparent research gaps, especially in the user-focused studies emphasized in the paper.

Keywords: dark net; systematic literature review; user studies; user perception; security and privacy

check for updates

Citation: Tazi, F.; Shrestha, S.; De La Cruz, J.; Das, S. SoK: An Evaluation of the Secure End User Experience on the Dark Net through Systematic Literature Review. *J. Cybersecur. Priv.* **2022**, *2*, 329–357. https://doi.org/10.3390/jcp2020018

Academic Editor: Xavier Bellekens

Received: 1 April 2022
Accepted: 10 May 2022
Published: 27 May 2022

1. Introduction

The World Wide Web is a network of linked hypertext files that can be classified into three regions: surface web, deep web, and Dark Web [1]. The surface web is accessible to all users of the Internet. Many users and researchers also refer to it as the open web. It consists of all the websites that have been indexed and crawled, thus making it accessible through DNS lookups, search engines, and internet browsers, such as Google Chrome, Internet Explorer, or Firefox [2]. On the other hand, the deep web is the collection of websites that search engines do not index, and these are usually hosted on private databases, the back end of the surface web's websites, such as websites that require authentication, academic journals, and other out of reach content. Finally, the Dark Web, a portion of the deep web, consists of websites that only specialized web search engines can access [3]. Rudesill et al. estimate the deep web, which houses Dark Web or Dark Net, to be about 400–500 times bigger than the surface web. Their paper further describes Dark Net as a flourishing space for illegal, problematic, and sometimes dangerous activities [4]. The Dark Web consists of several interlaying networks forming the Dark Net.

Created as an isolated set of networks from The Advanced Research Projects Agency Network (ARPANET), Dark Net refers to the subset of the deep net that has hidden network traffic [5]. Unlike the Surface web or Internet, where servers store and facilitate the websites, Dark Net websites are hosted in private networks between trusted peers. These peers or volunteers run relays and nodes that enable these private networks' traffic.

Furthermore, these networks can only be accessed with specific software, configurations, and authorizations, thus making it difficult for anyone to monitor or track users on the Dark Net.

In this way, Dark Net provides a haven for users that want to maintain privacy in their online activities [6]. Although the general media often view Dark Net as a source of malicious activities and a platform full of threat actors and ill-disposed hackers, the reality is more nuanced [4]. Ehsan et al. concur that Dark Net is also a source of new information and a meeting ground for journalists, human rights activists, political dissidents, whistleblowers, as well as scholars [7]. With ever-growing users and content on the Dark Net, it is imperative to understand the security and privacy threats that users might face while interacting within the Dark Net. It is also critical to note that Dark Net can be accessed through specific software and tools such as Tor, a browser implementing onion routing and bounces communication over a network of relays run by volunteers to allow access to the Dark Net. Subsequently, due to the network structure of Tor, it provides some level of anonymity for the users. According to Mirea et al., in January of 2018, there were an estimated 4,000,000 users on Tor visiting the Dark Net [6].

Creating a platform for anonymity undeniably attracts malicious actors to the surface of the Dark Net. Unfortunately, however, various users utilize the Dark Net, which includes:

- Users intend to conceal web browsing to circumvent internet-activity monitoring by local ISPs (Internet Service Providers) or law-enforcing government agencies. These users can include people from legitimate backgrounds such as journalists or whistle blowers [6,8]. However, these users can also include criminals who intentionally use these services to conceal their identities. It is challenging to provide selective anonymity without compromising on the anonymity network in the first place, making other legitimate users vulnerable to the system.
- Users seek encrypted communication with an immediate network, concealing logs of chat or instant messages being documented on a database. These users might need the protected network not only for anonymous communication but also for financial transactions.
- Users seek to publish controversial journalistic articles amid an oppressive regime. This is a specific user base as there have been several incidents where journalists and whistleblowers were targeted after their identities have been revealed https://carleton.ca/align/2019/illuminate-exploring-the-dark-web-a-cloak-for-journalists-and-their-sources/ (accessed on 1 December 2021).

Due to its anonymity feature and lack of policing, Dark Net markets have been flourishing. With the advancement of technology, Dark Net is becoming more accessible to general population. In this scenario, there is a chance that users who are not aware of the threats and risks associated with Dark Net might fall trap to criminal activities or traps set by various police agencies. As described by Masson and Bancroft in their paper, Dark Net is a growing cryptomarket for exchange of illicit drugs within the users which is not sort of scams, traps, hackers, and threats [9]. Privacy and security are part of the fundamental drivers for users to adopt the Dark Web [10], which has motivated our research to understand and analyze the existing research studying different aspects of privacy and security of the Dark Net, including but not limited to the illegal markets hosted in the Dark Web, the deanonymization techniques of Dark Net users, the attack landscapes, as well as the existing user studies since users are a critical component to the Dark Net architecture [11]. By examining the distinct aspects of Dark Net security and privacy, a comprehensive analysis of these aspects will contribute to the countermeasures taken to defend against malicious activities on the Dark Net promoted by unethical users. Accordingly, it is crucial to analyze and understand the inner workings of the Dark Web, including its users' activities to help countermeasure and mitigate malicious activities.

Restrictions and limitations for directly browsing the Dark Net for this research determined that a systematic evaluative approach of related literature can be appropriately suited to the premise of a secure end-user experience. In that regard, we conducted a systematic literature review to provide a holistic overview of the existing literature in this field, which has been confirmed to be of excellent value in other domains [12]. The systematic review conducted in this research seeks to resolve a qualitative evaluation of secure end-user experience on the Dark Net. We collected 2693 in research articles related to the Dark Net's privacy and security. After the final exclusion round, 200 papers from the initial corpus were further analyzed and categorized into different themes after exhaustive thematic analysis. We found that out of 200 articles analyzing the privacy and security of the Dark Net, only 9 conducted any user studies. Thus, given the focus of our research, we performed an in-depth analysis of 9 papers that focus on the user factor. Even those studies that conduct user studies primarily focus on the anonymity network and do not detail user concerns of Dark Net usage, reasons for using Dark Net, or whether the users have any expertise in using such critical network platform where several malicious actors can misuse the lack of knowledge from the user's side [13].

There is an increase of Dark Net usage among general users, in addition to threat actors, whistle blowers, journalists, and policing bodies, because of the anonymity the Dark Net provides [14], in these circumstances, it is crucial to review the research conducted so far and to study the gaps in the knowledge that need to be further explored. More importantly, as researchers, we should study the privacy and security aspects of the Dark Net usage to aid nonmalicious users in these platforms. Thus, the need to understand the body of work conducted so far in this field and to drive future work towards analyzing privacy and security aspect of Dark Net usage from a user's perspective has motivated our paper.

This systematic evaluation is critical in understanding user privacy and security on the Dark Net. Furthermore, the specific search methods have recognized the user focus and the gaps in the literature, which will benefit the research community in learning more about this under-researched user experience domain. In summary, the main contribution of this paper is as follows:

- Provide a comprehensive overview of all themes and subjects explored so far in Dark Net research;
- Highlight the importance of the study of privacy and security in the Dark Net from the user's perspective;
- Point out the gaps and less studied themes in Dark Net research.

In the following sections, we discuss our method of collecting these papers as described in Section 3. In the next Section 4, we explore the results of the 200 papers, which detail the technical aspects of the Dark Net and the technologies required by the users before using such platforms. After that, we detail the user studies in Section 4.2, mention the limitation and future extensions of this work in Section 6, and finally conclude the paper by summarizing the content in Section 7.

2. Related Work

The Internet consists of websites and web-based content that search engines do not index or crawl either by design or for privacy. These websites and content form the deep web, which remains hidden to a user operating a standard web browser. The network layer of the Dark Web forms the Dark Net; as Zhang & Zou describe, the Dark Net is a part of the deep web, which is an encrypted and private network that requires dedicated and specialized software (such as Tor) for access. This type of network allows users to remain anonymous and makes their network activity untraceable [15]. Dark Net provides anonymity which may attract a variety of users such as whistle-blowers, journalists, users seeking privacy, threat actors, and hackers [16]. The majority of the research has focused on the illegal use of the Dark Net. Along these lines, Lusthaus uses data collected over seven years to analyze the types and extent of cyber-crime conducted within the Dark Net [17]. However, it is also essential to study and analyze the importance of user experience on the Dark Net. Many users might be exposing themselves to security vulnerabilities while interacting on the Dark Net. Unlike the surface web, the Dark Net poses as a safe and private environment, which might make users feel more secure sharing information that they otherwise would keep to themselves. However, this type of uninhibited activity can lead to danger because, as Ehsan et al. discuss in their paper, when correct tools are employed, it is not so difficult to link real identities to the Dark Net user profiles [7].

There are many specialized Dark Net surfing systems available today; some examples of these systems are: The Onion Router (TOR), Free-Net, Invisible Internet Project (I2P), Java Anonymous Proxy called Jon Do (JAP), and so on. The two most popular among these systems are TOR and I2P. Although both of these systems provide the same functionality, which explores Dark Net anonymously, the main difference lies in implementing the systems. As Ali et al. lay out in their paper, Tor uses at least three nodes (devices) to relay encrypted messages to prevent traceability and preserve anonymity. In contrast, I2P creates a virtual network between the sender and receiver of the message, which cannot be tapped by a third party like an internet service provider [18].

We also see that several prior studies emphasize the importance of understanding the user experience on the Dark Net or Tor [8,19]. Additionally, although it appears that the Dark Net provides better privacy than the surface web with ever-changing servers and encrypted networks, it still poses risks, especially for users who possess limited cyber-security knowledge and skills. User experience is central to understanding the security and privacy aspect of technology. Today, many platforms use aggregated user behaviors, decisions, and opinions to guide users to make informed decisions. Such a system provides a peek into user experience, which can help support end-user privacy and security management [20]. In their paper, Chalhoub et al. also employ a user experience study to navigate the security and privacy aspect of smart home devices [21]. Liu et al. also argue that the success or failure of security mechanisms is dependent on user behavior and experience. If users do not feel motivated to adopt the security mechanism or are unable to understand it, the said mechanism fails [22]. Hence, user focus is integral in studying a platform's security and privacy aspects.

To understand further, we conducted a Systematization of Knowledge (SoK) to provide a consolidated analysis of the user focus on Dark Net privacy and security research. A systematic literature review provides a succinct summary of all the research work conducted on a particular topic [23]. Such review papers are beneficial to inform readers of all the researched and reviewed information available on the topic and guide future researchers to look into the research gaps. For example, the works of Stowell et al. and Noah & Das provide a detailed analysis of research in the mHealth interventions for vulnerable population [24] and about online education through augmented and virtual reality installations, [25] respectively. In a similar vein from a methodological perspective, this paper attempts to provide a complete view of all the work conducted to understand the Dark Net's security and privacy. Although we could not find any systematic literature reviews adhering to our research topic, we found some literature analysis focusing on Dark Net evolution. The majority of the literature reviews published in security and privacy in Dark Net focus on the specific Dark Net forums and Dark Net markets, providing information on different cyber threats and hacker activities [26–28].

3. Methods

In order to categorize and understand the existing research on the deep web and Dark Net privacy and security, we conducted a systematic literature review. We reviewed these articles intending to answer the following four research questions, each with a list of keywords to narrow down the search:

- RQ1: What is the current research landscape for the Dark Net from the privacy and security perception of user data?
- RQ2: What are the technical security and privacy vulnerabilities of the Dark Net detailed by prior studies, and what are the mitigation measures suggested? Are these mitigation measures successful in user-focused vulnerabilities over the Dark Net?

- RQ3: How are prior research studies comprehending the privacy and security concerns of the users? For example, are there any user studies conducted to understand users' risk perception?

3.1. Database and Keyword-Based Search

We searched through six digital scholarly databases: Google Scholar, ACM Digital Library, ScienceDirect, SSRN, IEEE Xplore, and Sagepub. Our selection process was based on iterative evaluation. We started by defining appropriate keywords for our research. The search terms were identical throughout the six digital libraries and included the following terms: "Privacy"OR "Security"AND "Deep Web"OR "Dark Web"OR "Dark Net"OR "Deepweb"OR "Darkweb"OR "Darknet".

3.2. Inclusion and Exclusion Criteria

Our selection standards for the corpus required that all papers be: (1) research papers or articles published in peer-reviewed journals or conferences to best ensure academic integrity; (2) published in English—therefore, we did not use any translation software to convert the papers published into other languages; (3) made available by 31 August 2021. These selection criteria were chosen to ensure all papers were held to a high academic standing and could be accessed and analyzed by our research team. Moreover, papers were excluded if: (1) the full text was not available despite having privileged administrative access. For these papers that were not available for open access, we reached out to the authors via email to gain access to the full text; (2) they were presented as a work in progress, posters, extended abstracts, or any other form apart from a complete paper; (3) the content analysis showed that the research was not directly related to Dark Web or deep web privacy and security; (4) the collected articles were part of book chapters. At the end of this step, we had 1751 in papers. As we detail the data collection, screening, and paper analysis stage in the following subsections, we provide a snapshot of the steps in Figure 1.

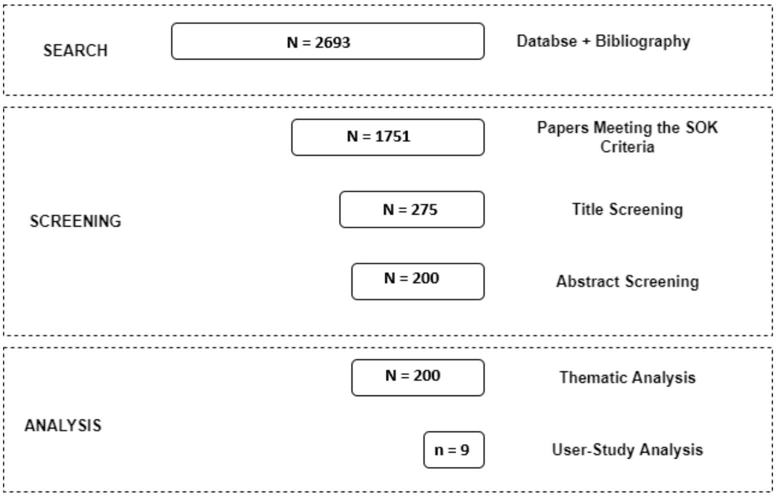

Figure 1. A snapshot of the data collection, screening, and analysis methodology along with the $n =$ # of papers screened in each stage of the literature review.

3.3. Title and Abstract Screening

We conducted a manual title and abstract-based screening to remove any irrelevant papers. During this screening process, some papers were excluded. These were articles about privacy or security that were not directly related to the deep web or Dark Web and papers that examined the Dark Web but were irrelevant to privacy or security. After performing the steps mentioned above, a total of 275 articles remained for a detailed analysis. Additionally, the full-text analysis further reduced the literature count by 75, leaving us with a corpus of $N = 200$ papers.

3.4. Thematic Analysis

We conducted a detailed thematic analysis to synthesize the knowledge from prior literature. For this, we followed the qualitative analysis techniques as explained by McInnes et al. [29] and Moher et al. [30] in their papers. For this analysis, we looked into the abstract, methods, results, discussion, and conclusion of the $N = 200$ collected papers, obtained from the title, abstract, and full-text screening. The papers were then evaluated by first going through each one and generating the codebook. The codebook consisted of 107 open codes, which were themed into ten overarching themes, including frameworks and technological solutions proposed, network analysis, deanonymization, the attack landscape on the Dark Web, forensic studies, evaluation of illegal activities on the Dark Web, ethical and legal implications of research, author notes and overviews and evaluations of the Dark Web, studies on Dark Web illegal markets, forum, and social network studies, and finally, the user studies. The codebook details with the open codes and themes are provided in Table 1.

Table 1. A snapshot of the correlated open codes and themes generated for thematic analysis of the analyzed 200 papers on dark net user privacy and data security.

Theme	Open Codes
Frameworks and Technological Solutions of Dark Net Privacy and Security	Dark Net Monitoring, Framework Based on Hidden Markov Models, Automating Traffic Analysis for Securing Network, Solutions of User Deanonymization Problem using Artificial Intelligence, TOR Crawling, and Classification, Image Analysis, Bag of Visual Words, Topic Detection Model, Stochastic Analysis, Machine Learning to Predict Threats, Real-time Alert System, Profiling Dark Net Data, Probabilistic Model, Graph Modelling, Tor Ranking Algorithm, Online Processing Algorithm, Graph Mining, Probabilistic Pre-processing Model for Data Sanitization, Dark Net Application Suite Using Cryptography, Random Walk Algorithm, Agglomerative Clustering, Malicious Dedicated Hosts Detection, Data Mining, Modeling and Querying the Dark Web, Zeronet Crawling, Dark Net Design, Attack Resistant Network Embedding, Image Analysis, Greedy Embedding Algorithm, Freenet Routing, Smart Contracts, Bloom Filters
Network Analysis of the Dark Net	Traffic Monitoring, Traffic Classification, Taxonomy of Dark Net Traffic, Tor Traffic Analysis, Traffic Misconfiguration, Port Scanning, P2P Network Routing, Hybrid Honeypot Architecture for Coverage of Large IPv6 Address Spaces, Network Monitoring using Topological Data Analysis, Network Telescopes, Passive Monitoring of Traffic, Probing Campaigns, Improper Traffic Analysis, Hierarchical Classifier of Dark Net Traffic, Freenet Routing, I2P Network
Attack Landscape	Worm Tomography, DDOS Attacks detection, Malware Analysis, Phishing Study, Tor Attacks, Cyber Threat Prediction, Real-time Malware Activity Detection, Tor Threat Analysis, Enterprise Level Cyber Attacks, Ransomware, Fingerprinting Dark Net Traffic Logs to Detect Malware, Emerging Novel Attacks, Distributed Reflection Denial of Service Attack Detection, Cryptocurrency Attacks, Blockchain Privacy
Dark Web Illegal Market	Single Vendor Marketplace Similarities, Dark Net Marketplace Vendor Accounts Linking, Identity Crime Prevention and Trading on Dark Net Marketplaces, Law enforcement Interventions Against Dark Net Market, Silkroad, Transactions in Cryptocurrency, Trust Logistics and Conflict Factors
Theoretical Overviews of Dark Net Privacy and Security	Tor V3 Services, Tor Attacks, Tor Security, SOK on Illicit Markets, Dark Web Privacy, Cybercrime Ecosystem
Evaluation of Illegal Activities Over Dark Net	Drug Trade, Identity Crime, Child Abuse, Criminal Activity
Forum and Social Network Studies Evaluating Dark Net Data	Forum Analysis on Suicide, Dark Net Forums Data Analysis, Forum Study on Law Enforcement Interventions Against Dark Net Market, Representations of Drug Users' Ways of Life, Sentiment Analysis, Authorship Attribution
Deanonymization of Dark Net Users	User Deanonymization, Tor Deanonymization, Tor Identity location leaks, Deanonymization Techniques, Personally Identifiable Information Data Mining, Geolocation, Deanonymization of Users Through Bitcoin Transactions, Drug Trafficker Identification, Location Leak
User Studies	User Behavior on Tor, Drug Cryptomarket Users, Silkroad Users, Internet Freedom, Revocable Anonymity to Abusive Users, TOR Community Motivations, Dark Web Perceptions of Students and Parents
Ethical and Legal Implications of Dark Net Transactions	Legislative Limits, Tor Legal Issues, Chatbot, Slovenian Legal System, Legal Enforcement

Table 2 in the results section shows the distribution of the papers as per the thematic analysis. Any paper which had any form of user study, even if that was not the primary theme of the paper, was marked in the user study category. This was mainly done given the focus of the research. The codes were not mutually exclusive, and the papers detailing any of the earlier themes were categorized accordingly. The first author of the paper performed the thematic analysis. If there was any confusion about the categorization, then the second and third authors of the paper helped in the thematic analysis of the work until all three authors agreed on a theme. All three authors reviewed the final thematic evaluation to check for discrepancies or disagreements.

Table 2. Thematic overview of the papers collected and analyzed based on the codebook and themes generated. Note that the total of the percentages is over 100 since the categories are not mutually exclusive.

Category	Articles
Frameworks and Technological Solutions	54 (27%)
Network Analysis of the Dark Net	49 (24.5%)
Attack Landscape	30 (15%)
Dark Web Illegal Market	25 (12.5%)
Theoretical Overviews of Dark Net Privacy & Security	20 (10%)
Evaluation of Illegal Activities Over Dark Net	18 (9%)
Forum and Social Network Studies Evaluating Dark Net Data	17 (8.5%)
Deanonymization of Dark Net Users	13 (6.5%)
User Studies	9 (4.5%)
Ethical and Legal Implications of Dark Net Transactions	7 (3.5%)

3.5. User Study Analysis

After the thematic analysis, we conducted a detailed user study analysis focused on the $n = 9$ user studies. We expected more papers on the user studies, but we could only find nine relevant papers in the data repository after careful evaluation. After that, we extracted the quantitative and qualitative findings to assess the user perspective on the security and privacy of the Dark Web and deep web research conducted by prior studies.

4. Results

For each of the 200 papers in our corpus, information was collected, classified, and analyzed separately by categorizing the corpus papers into ten themes, as shown in Table 2. This section outlines the results pertaining to this thematic analysis. First, we mainly looked into the methods, results, discussions, implications of the mentioned papers and the timeline of paper publications which can be seen in Table 3. We then performed a detailed analysis of the user studies, discussed in the later sections.

Table 3. Summary of the timeline of the papers by themes. All papers were published after the year 2005.

Year (20–)	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**
Frameworks & Technological Solutions	1	-	-	1	-	1	2	2	2	3	3	3	4	3	8	10	5
Network Analysis	-	1	-	1	-	1	-	4	1	2	2	4	5	10	7	3	5
Attack Landscape	-	-	-	3	-	-	1	-	-	3	2	2	2	4	3	5	-
Illegal Market	-	-	-	-	-	-	-	1	1	1	-	1	2	4	7	5	3
Theoretical Overviews	-	-	-	-	1	-	1	-	1	-	1	1	4	2	4	4	1
Illegal Activities									1	1	-	2	-	5	3	5	1
Forum Studies	-	-	-	-	-	2	-	1	1	-	-	2	1	2	3	5	-
User Deanonymization	-	-	-	-	-	-	-	-	-	-	-	1	-	3	2	5	1
Ethical & Legal Implications	-	-	-	-	-	-	-	-	-	-	1	1	1	2	1	1	-

4.1. Thematic Analysis

4.1.1. Frameworks and Technological Solutions of Dark Net Privacy and Security

Over a quarter of the papers 54 (27%) aimed to design and introduce technology-based solution as well as frameworks to enhance the privacy and security of the Dark Net [31–36,36–77]. The research was based on several types of technological solutions proposed by the authors to enhance the privacy and security of the Dark Net, including artificial intelligence approaches, data mining, network-based solutions, encryption, as well as statistical approaches as shown in Figure 2. Many of the papers use these technical solutions, the most prominent of which is combining network-based solutions with artificial intelligence methods. One such study, "ToRank: Identifying the most influential suspicious domains in the Tor network", develops a new algorithm for classifying the onion domains into normal and suspicious activities, then ranking these domains and identifying the influential ones. Through their study, AL-Nabki et al. also extended the version of the "Dark Net Usage Text Addresses" dataset up to 10,367 manually labeled hidden services in the Tor network [58]. Fidalgo et al. attempt to classify images uploaded to the Tor network using artificial intelligence methods in a different approach. These methods include semantic attention key point filtering, which is a model introduced in this paper to eliminate non-significant features which do not belong to the main object of interest in the image at the pixel level [38]. Figure 3 shows a detailed timeline of publications of papers related to the theme of frameworks and technological solutions for Dark Net privacy and security. This timeline demonstrates the growing awareness and subsequent study of privacy and security in Dark Net research.

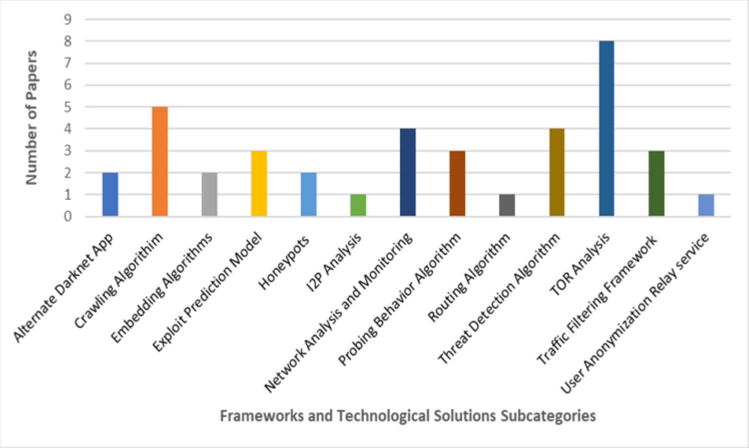

Figure 2. A snapshot of different frameworks and technology solutions of Dark Net privacy and security discussed in the papers.

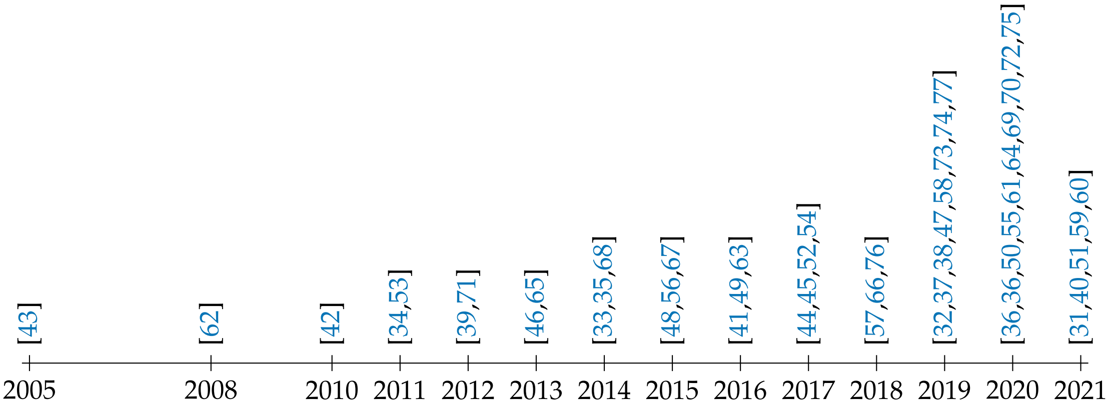

Figure 3. A timeline of different papers within the frameworks and technological solutions theme.

4.1.2. Network Analysis of the Dark Net

We classified papers as network analyses of the Dark Net if the methods adopted to investigate and analyze the Dark Net networks, such as traffic monitoring, traffic taxonomy, port scanning, network topology, and so on, as demonstrated in Figure 4. We found 49 (24.5%) papers in our corpus that fit into this category [78–124]. These papers provide insight on the workings and structure of the Dark Web networks. In this regard, Platzer et al. use traffic analysis methods to deanonymize hidden services on the Tor network. By analyzing traffic on the introduction point circuit data channel, Platzer et al. provide three independent methods that allowed them to deanonymize any hidden service on Tor [123]. In a similar approach, Vichaidis et al. investigate the cause of instabilities in transmission control protocol traffic of the Dark Net at different timescales. Analyzing the traffic instabilities daily allowed them to detect the large-scale anomalous event, while analyzing the hourly traffic allowed them to detect the small-scale anomalous events [85]. On a different note, we notice that the publications for this theme peaked at ten papers in 2018, from where it went down to 7 papers in 2019 and 9 papers between the years 2020 and 2021; Figure 5 provides further details on this trend.

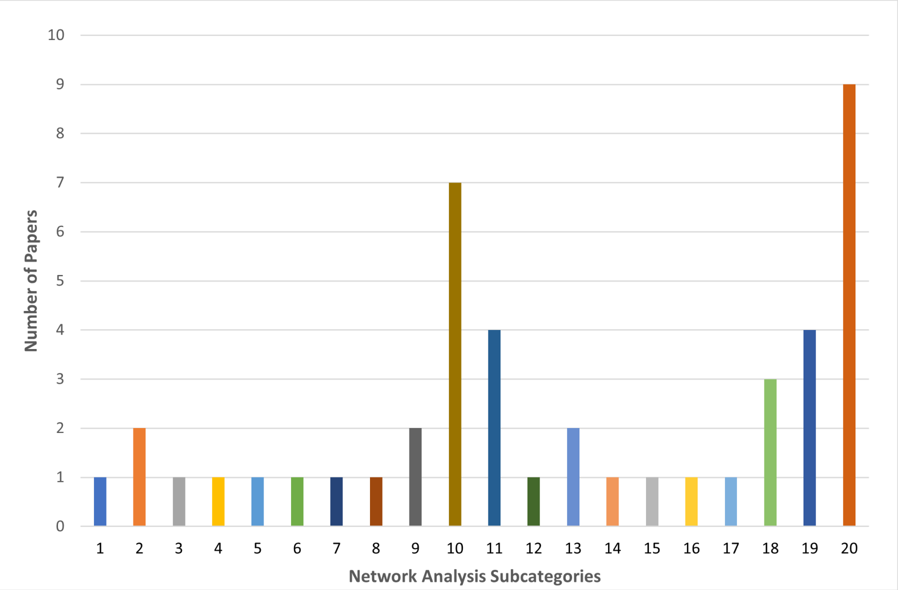

Figure 4. A snapshot of different themes discussed regarding network analysis of dark net privacy and security discussed in the papers.

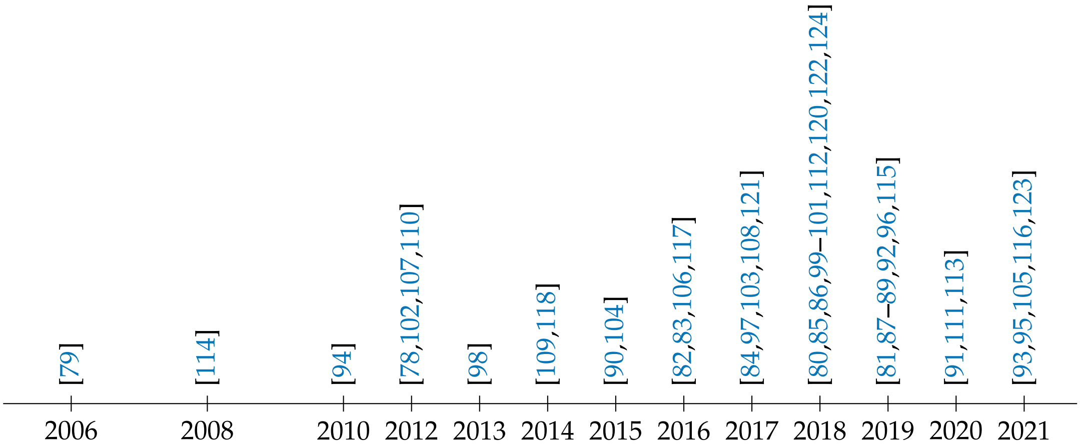

Figure 5. A timeline of different papers within the network analysis theme.

4.1.3. Attack Landscape

We classified papers discussing Dark Net privacy and security as attack landscape and scope of cybersecurity threats. We primarily focused our evaluation on seeing if the authors analyzed attack surfaces on the Deep Net or if they identified vulnerabilities or threats using Dark Net data or technology used to access Dark Net. In our analysis, we found 25 (12.5%) out of 200 such papers in our corpus [63,75,76,113,121,125–144]. These papers particularly describe the methods used to detect, prevent, mitigate, or predict cyber attacks. One such paper introduces a monitoring system used to detect Distributed Denial of Service (DDoS) attacks by monitoring the packet traffic on the Dark Net [63]. Similarly, Almukaynizi et al. designed a system that leverages Dark Web and Deep web data to detect cyber threats targeting crypto-currency users and platforms [134]. The bar graph Figure 6 demonstrates different attack vectors discussed in the 25 papers and their distribution among these papers. On a different note, we notice that the publications for this theme started in 2008 with three papers that year, but there was only one paper published between 2008 and 2014; we were unable to find any papers published in 2021 relevant to this theme (Figure 7).

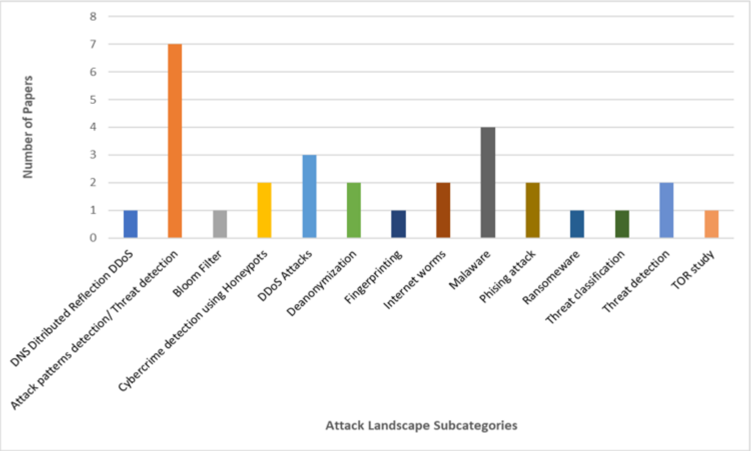

Figure 6. A snapshot of different attack vectors discussed by prior researchers with the distribution of papers for each subcategory.

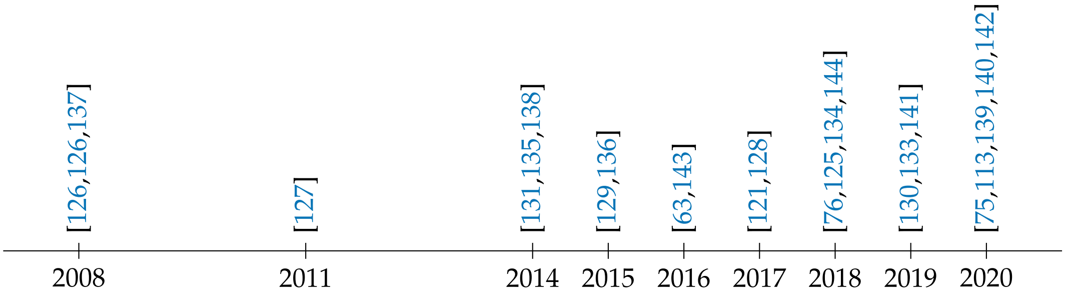

Figure 7. A timeline of different papers within the attack landscape theme.

4.1.4. Dark Web Illegal Market

Of the 200 papers analyzed, 23 (11.5%) studied Dark Web illegal (black) markets. These papers particularly explore the deep web marketplaces and utilize data from these markets for their investigations [14,17,36,73,74,80,102,145–162]. Some of these papers investigate the security of the financial assets of users of the Dark Web marketplaces, while others explore the criminal activities in the Dark Web marketplaces. The chart provides a good summary of these different themes discussed in the literature Figure 8. Of these, Yannikos et al. describe a method to monitor product sales in Tor marketplaces that leverages bitcoin transactions [151]. On a different note, Wang et al. introduce a method to link Dark Web vendors' different accounts through photo analytics, exploiting the unique photography styles of each vendor [161]. Furthermore, the first publication for this theme we were able to find was in 2012, where the publications were moderately steady over the years, except in 2019, where we found the largest number of publications with 7 papers (Figure 9).

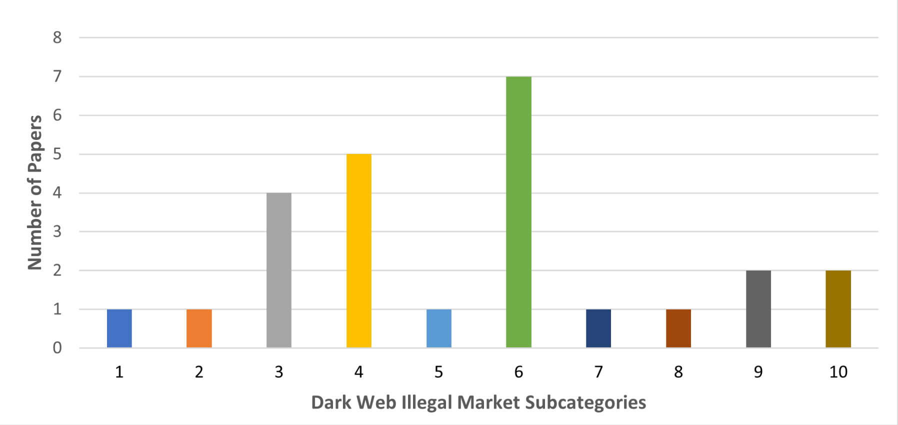

Figure 8. A snapshot of different Dark Web illegal market themes discussed by prior researchers with the distribution of papers for each subcategory.

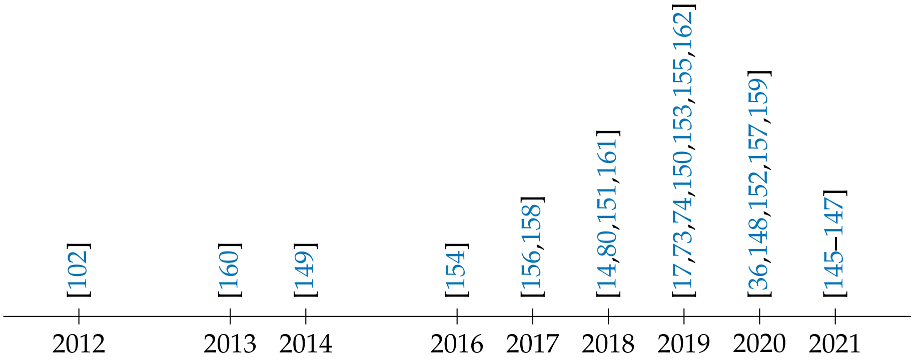

Figure 9. A timeline of different papers within the illegal market theme.

4.1.5. Theoretical Overviews of Dark Net Privacy and Security

Of the 200 papers analyzed, we considered 20 (10%) papers as theoretical overviews of the Dark Net privacy and security [163–182]. These papers include works which consolidate the prior research on Dark Net privacy and security, by addressing the current state of privacy and security in the Dark Net, as well as the tools and technology exclusive to the Dark Net.

We also included papers in this category if they compiled and introduced various techniques and ways users can protect their privacy and be secure while using the Dark Web. Along these lines, Ranakoti et al. present a multitude of approaches and techniques to protect Dark Net users through anonymity [171]. In their paper, Hatta also examined anonymity in the Dark Net, as well as the different technologies used to access the Dark Web, but mainly focused on anonymization by Tor [173]. Further, the first publication for this theme we were able to find was in 2009, when the publication was moderately sparse over the years, until 2017 when the number of publications would rise and maintain a steady pace until 2021 (Figure 10).

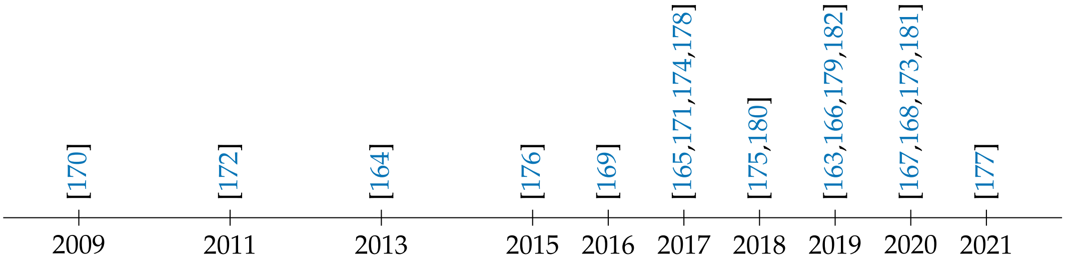

Figure 10. A timeline of different papers within the theoretical overviews of dark net privacy and security theme.

4.1.6. Evaluation of Illegal Activities over Dark Net

Papers were classified as an evaluation of illegal activities over the Dark Net when they reviewed the presence as well as impacts of illegal activities on the Dark Web in general and its illegal markets in particular on the users [9,10,64,139,152,155,160,183–193]. Of the 200 papers in our corpus, 18 (9%) papers explored the illegal aspect of Dark Net activities. In that regard, in their paper, Witting discusses the ethics behind allowing the police to distribute illegal child sexual abuse materials in order to be able to infiltrate similar circles on the Dark Net and weighs the pros and cons of establishing the legality of such practices, especially on actual victims and future probable victims [187]. On the other hand, He et al. propose machine learning classifiers to categorize illegal activities on the Dark Net. This is achieved by selecting laws and regulations pertinent to diverse types of illegal activities to train their classifiers [183]. Moreover, the majority of the papers (75%) within this theme were published between 2018 and 2020. Unfortunately, we could find only one paper published in 2021 before our data collection ended. Figure 11 shows more details of the publication timeline of this theme.

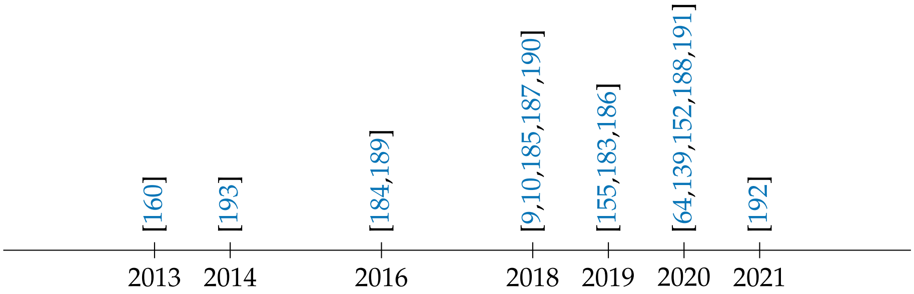

Figure 11. A timeline of different papers within the evaluation of illegal activities over the dark net theme.

4.1.7. Forum and Social Network Studies Evaluating Dark Net Data

The papers that focused on the analysis of content shared by users in the Dark Net across forums and social network platforms make up 8.5% (17 papers) of the papers used in this review [9,16,70,71,184,194–205]. These papers employ techniques to classify and analyze the messages shared by the users to gauge the mental model of the user, as well as to predict any cyber threats. For example, Almukaynizi et al. describe a social network analysis that can identify malicious activities and help predict potential cyber threats by scanning the content shared across Dark Net forums [199]. Similarly, Park et al. use data collected from the Dark Net forums to conduct a sentiment analysis that shows the correlation between negative sentiments of users and real-world terrorist events [200]. We also note that the publication for this theme started in 2010 with two different papers, but there were only two papers published between the years 2011 and 2015. We were unable to find any new papers pertaining to this theme published in 2021 (Figure 12).

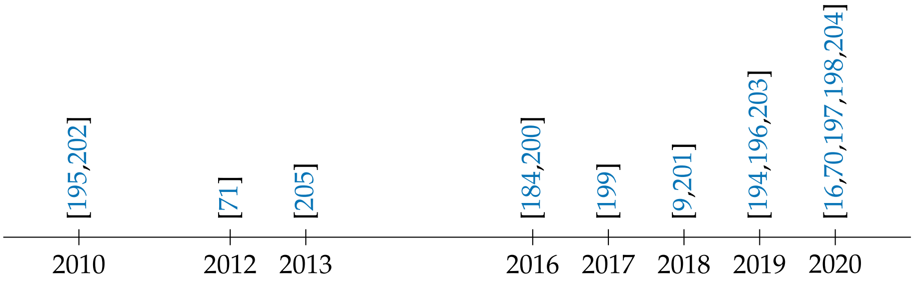

Figure 12. A timeline of different papers within the forum and social network studies theme.

4.1.8. Deanonymization of Dark Net Users

Thirteen (6.5%) papers out of two hundred focus on the promise of anonymity provided by the Dark Net [7,69,122–124,162,168,206–211]. Mainly, the Dark Net attracts users who want to be able to share their information in privacy while remaining anonymous and untraceable. However, anonymity is not a given on the Dark Net. Arabnezhad et al. introduce a tool that links Dark Net aliases with aliases used in the standard web, which in turn allows for identity detection of Dark Net users who create posts on both Dark Net and surface net forums [7]. Some papers study the intentional trade of Personally Identifiable Information (PII) within the Dark Net forums. Lin et al. provide a framework in their paper that can help identify partial PII shared by users in the Dark Net forums, thus helping authorities protect these PII for at-risk population [208]. Additionally, the publication of papers within this theme started in 2016, with publications in 2020 alone accounting for half of the papers analyzed in this study (Figure 13).

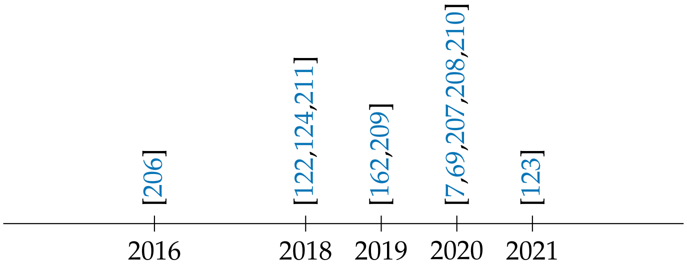

Figure 13. A timeline of different papers within the deanonymization of dark net users theme.

4.1.9. Ethical and Legal Implications of Dark Net Transactions

Only 7 (3.5%) papers studied in this review discussed the ethical and legal implications of Dark Net transactions [4,10,72,187,212–214]. As a result of the anonymous and untraceable nature of the Dark Net, it attracts threat-actors that can conduct activities of an illicit nature without the fear of impunity from the authorities. The Dark Net websites and forums create a dilemma for the authorities to uphold legal and ethical standards in the Dark Net discourse. Mihelic et al. discuss the limitations of legal enforcement when policing illegal activities such as the distribution of child pornography, illegal trafficking of arms, drugs, illegal items, or personal information. Although the paper focuses solely on the measures used by Slovenian Police authorities, which involves using malware to trace the threat actors, the theme of ethical implication applies to all policing bodies across other nations as well [212]. The current legal systems are not prepared to police the activities on Dark Net and thus often have to resort to means that might otherwise be considered unethical. On the other hand, Jardine argues through his paper that the current image of the Dark Net might lead to an eventual shutdown of the current form Dark Net thus leading to a more restricted and emboldened version of it that might be even more difficult to manage [10]. We notice that starting in 2015; there was an average of one paper published within this theme per year, except for 2018 where two papers about ethical and legal implications were published (Figure 14).

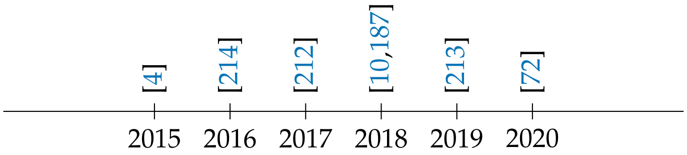

Figure 14. A timeline of different papers within the ethical and legal implications theme.

4.2. Analysis of User Studies

In addition to our thematic analysis, we performed a detailed analysis of our corpus's user studies ($n = 9$). Our goal was to understand and assess the studies that evaluated user perceptions of privacy and security on the Dark Net. Therefore, we performed a thorough analysis of the $n = 9$ user studies. In addition, we analyzed some of the study aspects, such as the type of study conducted, study populations, and context of the study. Specifically, we wanted to analyze the themes studied via user studies in these papers. Although, as we have pointed out previously, users play a significant role in the Dark Net study, through these papers, we wanted to understand the current trend in the focus of such user studies in this research landscape.

4.2.1. Study Method

Of the $n = 9$ user studies in our corpus, 5 (55.56%) were qualitative studies [6,9,184,193,205] with open-ended questions, three of these papers consolidated their user studies with forum studies. Of other studies, 3 were mixed method including some qualitative aspects as well as some quantitative analysis [215–217] and only one was exclusively qualitative [10] using respondent level data from the CIGI/Ipsos 2016 survey.

4.2.2. Study Population

Most of the user studies in our corpus had an insignificant number of participants, with Bancroft and Reid only able to recruit 5 participants from the Dark Web users [184]. The most participants any study had was 78 participants [217], except for Jardine, who used data from respondents of the CIGI/Ipsos 2016 survey [10] which gave them access to a survey of 17,121 participants, Table 4 presents this in more details.

It is important to note that only one paper [6] did not provide any demographic information on its participants in order to respect the culture of the Dark Net and guarantee total anonymity.

Table 4. Number of study participants for the different user studies.

	Qual Studies (5)	**Quant Studies (3)**	**Mixed-Method Studies (1)**
Participants			
>0, ≤10	2 (40%) [9,184]	0	0
>10, ≤20	2 (40%) [6,193]	0	0
>20, ≤50	1 (20%) [205]	1 (33.33%) [216]	0
>50, ≤100	0	2 (66.67%) [215,217]	0
>100	0	0	1 (100%) [10]

4.2.3. Recruitment Methods

Except for [10], the authors of the other papers recruited participants and collected their data. These papers used different types of recruitment methods. Some papers used more than one method to obtain the most recruits possible. The method used the most was via forum publication, as in [6,193,215], where only [6] specified the forums they used to publish their invitations. Authors also made use of social media [9,215], where they requested participation in their research. In the case, of [9] one participant approached an author via Twitter. A method equally used was word of mouth [9,184].

Additionally, the author made use of TOR-specific mailing lists in [215,216]. In one case, the message board recruitment of 'Silk Road' site members was used to recruit participants [205], and finally recruited students and their parents from a university in the province of Gauteng, South Africa. However, the authors of this last paper did not aim to recruit specifically users of the Dark Net since the purpose of the study was to analyze their participants' perceptions of the dark Net.

4.2.4. Study Categories

The user studies had a broad spectrum concerning the subject of each research. Two of these papers adopted a holistic aspect and sought to understand the perspective of different users of the Dark Net. As such, in their paper "The not so dark side of the Dark Net: a qualitative study" Mirea et al. tried to understand the mindset of established Dark Net users and surveying by posting a questionnaire link embedded in an invitation letter in four Dark Net hosted forums and ended up with 17 completed responses. The survey investigated how the participants found out about the Dark Net, why they used it, and the exciting features participants found appealing about it. Mirea et al. also asked their survey participants about their opinion on Silk Road and whether they think the Dark Net promotes crime [6]. On a similar note, Odendaal et al. examine the current levels of South African students' awareness, understanding, and utilization of the Dark Net and contrasts it to that of older generations, in this case, the students' parents [217]. The survey in both studies was similar in many aspects. However, the population was divergent as most of the participants in the second study were not regular users of the Dark Net.

Another exciting category of these user studies was illegal drugs on the Dark Net; 4 papers examined this subject from different lenses. Two of these papers only marginally addressed the security and privacy aspect of the Dark Net and its users and focused more on the drug element. One of these papers primarily focused on the illegal drug quality as perceived by Dark Net market users and how they compare drug quality [184]. Similarly, in their study, Masson and Bancroft only touched on privacy and anonymity marginally, as their main subject of interest was to conduct an ethnographic study on Dark Net drug centered markets; as such, no questions about privacy or security concerns were asked in this study, and privacy was only mentioned once by a participant as a non-concern [9]. The remaining papers chose the silk-road market as their primary object of study, with two different populations. While Van Hout and Bingham [193] targeted vendors exclusively in their study "Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading" , their previous paper "'Surfing the Silk Road': A study of users' experiences" addressed silk road buyers [205]. Both papers had a similar outline, with some questions being exclusive to the different populations of the studies.

In their paper, Huang and Bashir [216] scrutinize the motivations behind Tor network users volunteering their resources to sustain Tor services despite the risks, and they also examine the users' perception of the attitudes that the current social and legal system has toward the Tor network and the challenges they face. This paper shows that the predominant motive of these volunteers is to advocate and provide privacy for online users. On the other hand, Ref. [215] explored the reasons behind the differences in self-reported usage of anonymous networks to help them understand if users would be willing to change the way they use anonymous networks because of a new technical scheme.

5. Discussion and Implications

We conducted a detailed systematic review of 200 papers focused on the privacy and security of the Dark Net with an emphasis on the user side. We recognize and acknowledge the importance of the valuable research contributions towards improving the security and privacy of the Dark Web network; however, it is crucial to note that there are some identified research gaps through this literature review that can be further expanded to enrich this field. Thus, we need more studies to thoroughly comprehend the security and privacy challenges faced by the average Dark Net user. This section presents our recommendations for future directions in this research area based on our analysis of the papers.

5.1. Focus on Technical Aspects

Previous research on the Dark Net security and privacy tends to be primarily technical. Researchers focused on technical skills such as network analysis, web crawling, and artificial intelligence (AI) to preserve the privacy of users and safeguard their data on the Dark Net [31–33]. Some of these studies also discuss the use of automation in the detection of anomalies [31–33]. Another aspect of this research that we have noted is the feasibility of these technical solutions. Often these solutions include the use of AI or Machine Learning techniques which use datasets with bias issues that AI/ML algorithm creators seldom address in the implementation. As an extension of this research, we plan to obtain a representative sample that is understandably challenging to obtain given the nature of Dark Net data. We can discuss obtaining more representative samples to provide technical solutions as a research community.

Furthermore, the current research focuses on the network topology of the Dark Net, which, although highly critical, does not give much insight into the use of these networks. For example, there is little to no usage monitoring on the Dark Net [218], given the nature of access. However, due to the feasibility of access points such as Tor, more younger adults are moving to the platform, which can be concerning; thus, usage moderation from the access point perspective will be beneficial, such as that of Tor. Though it is essential to observe the Dark Net patterns and study the attack vectors, one of the vital components we often seem to ignore is the user side. The users of the Dark Web have been traditionally more technically sound [219]; however, with increasing access to tools like Tor, more technically diverse users are joining the Dark Net networks. Thus, it is imperative to understand the users we have mentioned in the following subsection.

5.2. Future Direction towards User Studies

In the previous subsections, we note the possible harmful effect on the users due to the Dark Net; hence, our primary focus in this study is to emphasize the user component of Dark Net research. However, from our analysis, we discover a significantly smaller number of user studies yielding only $n = 9$ papers on the given topic of research [6,9,10,184,193,205,215–217]. This clearly shows a research gap where the perceptions and experience of users' interactions within the Dark Net are concerned. This is even more concerning as prior studies have shown that several non-experts in technology use Dark Net for various interactions.

Additionally, policing agencies from different countries also monitor the interactions and transactions on the Dark Net. In such a scenario, users with little technical expertise and little or no data protection surfing the Dark Net websites present a troubling picture. Therefore, user studies provide a unique perspective on a situation that can provide valuable insight into users' experience navigating these networks. In the case of the Dark Net, user perception and experience play an even vital role because the Dark Net is built by the volunteer users base that facilitates the entire Dark Net network architecture and runs relays that ensure the anonymization of these users. Dark Net is used for multiple purposes, from whistleblowing [6] to sharing information to conducting illegal transactions and discussing real-world terrorist attack [220,221]. In this way, Dark Net provides a landscape that can be very useful and detrimental to modern democracy [222].

User experience and user-focus studies can help researchers evaluate emerging trends, technology evolution, and real-world impacts. It can also inform legal authorities to create legal reforms and policing measures and track criminal activities. However, even for the nine studies that conducted any user-focused experiments, two of them were generic. For example, instead of focusing on the Dark Net, they focus primarily on Tor, through which users access Dark Net. In addition, three of the user studies that managed to do an interview and participants' observations had less than 20 participants, as explained earlier. Moreover, the studied participants were primarily non-experts; thus, all the technical solutions the researchers are working on might not work for them unless user input is considered. As we see from prior studies in different domains, usability [223–225] and accessibility [226,227] play a vital role when it comes to the adoption of technologies. Especially for Dark Net, research by Morch et al. has shown fatal consequences of not looking into the user side [201].

We understand that participant recruitment can be a significant challenge for user-focused experiments, especially when it comes to sensitive technologies such as Dark Net. However, none of the papers discuss this constraint or emphasize how to address this issue. With over two million active users of the Dark Net and the sheer scale of illegal activities that can benefit from the under-laying network, it is essential to address this. Moreover, in lieu of illegal activities, it is also imperative to protect those whose usage is dependent on the anonymity of the network and help protect their identity.

5.3. Attack Surfaces

Another critical aspect of the Dark Net research is that despite the technological focus on the Dark Net, there are several attack vectors explored by the attacks. A simple example will be if a user uses identifiable information while using Tor or any such Dark Net access tools. However, research by Gallagher et al. showed how users often ignore these aspects and rely on the "black box" mechanism of tools such as Tor [228]. This is even more concerning as it creates a false sense of security [229,230]. Thus, in addition to the risk perception and evaluation of users [231], user education is critical as well [232]. We can adapt to Dark Net's previously studied and proven research techniques for this particular research area.

5.4. More Emphasis on Dark Net and Legal Implications

We noted that though our research and focus was on the Dark Net, most of the papers (98) focus on Tor or other gateway browsers or software, despite our best efforts. This is, of course, critical for this research. However, no paper focuses on the content of the Dark Net, Usage Statistics, or the type of user interactions. Thus, the emphasis on the Dark Net is essential, which is either left unexplored or little is known in the field. We acknowledge that given the type of data transactions, it is difficult to conduct the research; however, it is critical to understand the transactions done before protecting the user data. The more we know about it, the better it will be for the researchers to provide tools that protect users' privacy through anonymization and prevent data leaks when any interaction occurs through Dark Net.

Another benefit of focusing our research on the Dark Net will be to investigate the legal perspective. Much past research focuses on methods to track and gather evidence regarding specific criminal activities such as illegal trading of drugs and goods, illicit use of cryptocurrency, and other illegal activities [213,233]. However, there is little to no knowledge of the legal implications of regular Dark Net usage and interaction. This is especially concerning because of the heavy government surveillance and monitoring of these sites and that users are unaware of who they might be interacting with while on this sites [234]. In their paper, Rafiuddin et al. describe many precautions taken by the researchers before accessing the Tor websites to protect themselves from both law enforcement and the threat actors. This includes removing both microphone and webcam drivers from the machine, taping the webcam even after they have removed the drivers, using their VPN network, and completely removing all Personally Identifiable Information from the device [235]. However, an average internet user using the Dark Net to keep their activities private might not take these precautions and might get into trouble if they access fake sites created by law enforcement to trap criminals or fall prey to illegal trade chains. Thus, given this exciting take on the legal perspective, it is critical to explore this area to help the users prevent malicious interactions.

In summary, we propose that the larger research community explore more diverse avenues in the Dark Net research through this SOK. As pointed out above, we have highlighted four essential aspects of research that need to be studied in the future to gain a better understanding of Dark Net use. The benefits of outlining the research gaps are obvious; studying these less-explored topics will help the researchers and the overall user community understand the privacy and security risks of Dark Net use. Furthermore, this awareness will aid users from all walks to interact with this medium more carefully. The only drawback of studying these highlighted issues is that such studies might require more resources.

6. Limitations and Future Work

In this paper, we conducted a systematic analysis to evaluate the research articles and peer-reviewed papers published in the field of security and privacy of the Dark Net. We collected papers from six different digital repositories and limited our search to papers published in English. Therefore, we might have missed some papers outside of these digital libraries. However, our extensive literature review provides a detailed overview of the current research on Dark Net privacy and security, focusing on the user side. Additionally, the first author of the paper primarily performed the thematic evaluation. We addressed this by having all papers considered by the second and third authors in the last discussion. As for user studies, we only found 9 papers that included any user study analysis, despite our best efforts. We understand it is challenging to conduct user studies on such sensitive topics; however, even those papers are focused primarily on Tor than Dark Net.

This shows the research gap, and thus in the future extension of our work, we plan to conduct a literature review of user studies of privacy and security of the Dark Net using a specific keyword-based search. We also plan to contribute to the field by conducting user studies to evaluate the user perceptions and experiences of Dark Net usage while focusing primarily on a privacy and security perspective. In such a user study, we would like to compare the differences in perceptions and experiences of users based on their age group and technical abilities. This would also be an opportunity to review the privacy and security threats users face on the Dark Net and measure their awareness of these risks. The Dark Net's privacy and security risks are an apparent concern for the users, as shown through the different user study evaluations. As we acknowledge the difficulty in obtaining such user participation, we emphasize the criticality of understanding the perception of the Dark Net for any user, given the secretive yet vulnerable nature of the platform.

7. Conclusions

The Dark Net is an overlay network within the Internet that can only be accessed with specific software, configurations, or authorization through anonymization tools such as Tor, Freenet, or I2P. Although the Dark Net is often associated with illegal and criminal activities, it is an essential tool for many people looking for anonymity, such as journalists and politicians. Despite having the critical user component of the Dark Net, the user side of the Dark Net is severely understudied. To understand this further, we conducted a detailed systematic literature review after collecting 2693 papers from six different digital repositories, including ACM Digital Library, Google Scholar, SSRN, IEEE Xplore, and Sagepub. After that, we thematically analyzed $N = 200$ of the relevant papers on the topic. In these papers, we primarily examined the security and privacy of the Dark Net studied by prior literature. We found that current research focuses primarily on network analysis tools and methods for Dark Net security.

Additionally, papers discussing the technical aspects of the Dark Net privacy and security entirely focus on Tor. From the user side, it is also important to note that fewer than 5% of the papers in our corpus are user studies. Among those, two papers were broad-spectrum and only marginally touched on the security or privacy of the Dark Web. Thus, we see a need for more user studies and acknowledge the difficulty in obtaining the participant pool. Based on our analysis, we provide actionable recommendations based on the prior research, which paves the future direction of this research. This SoK on Dark Net privacy and security is critical to observing the research gap. This is one of the only papers to our knowledge that focuses on analyzing prior work on the user perspective of the Dark Net. This SoK also provides directions in the research area, which can be explored further to help protect the data of millions of Dark Net users.

Author Contributions: Conceptualization, S.D.; methodology, S.D.; validation, S.D. and F.T.; formal analysis, F.T.; investigation, F.T., S.S., and J.D.L.C.; resources, F.T., S.S., and J.D.L.C.; data curation, F.T., S.S., J.D.L.C., and S.D.; writing—original draft preparation, F.T., S.S., J.D.L.C., and S.D.; visualization, S.D.; supervision, S.D.; project administration. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: We have conducted a Systematic Literature Review (Systematization of Knowledge-SoK), which did not require any Institutional Review Board Review.

Data Availability Statement: The data collected in this work is the list of the papers, most of which have been mentioned in the this literature review.

Acknowledgments: We would like to acknowledge the initial contribution of Nathaniel Milliken, who started the project and collected the initial five papers on the topic. We would also like to acknowledge the Inclusive Security and Privacy-focused Innovative Research in Information Technology (InSPIRIT) Lab at the University of Denver, where this research was conducted. Any opinions, findings, conclusions, or recommendations expressed in this material are solely those of the authors.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alnabulsi, H.; Islam, R. Identification of Illegal Forum Activities Inside the Dark Net. In Proceedings of the 2018 International Conference on Machine Learning and Data Engineering (iCMLDE), Sydney, Australia, 3–7 December 2018; pp. 22–29. [CrossRef]
2. Huang, S.; Ota, K.; Dong, M. Web Usage Prediction and Recommendation Based on Web Session Graph Embedded Analysis. In Proceedings of the GLOBECOM 2020–2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
3. Schäfer, M.; Fuchs, M.; Strohmeier, M.; Engel, M.; Liechti, M.; Lenders, V. BlackWidow: Monitoring the Dark Web for Cyber Security Information. In Proceedings of the 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 28–31 May 2019; Volume 900, pp. 1–21. [CrossRef]
4. Rudesill, D.S.; Caverlee, J.; Sui, D. The deep web and the darknet: A look inside the internet's massive black box. *Woodrow Wilson Int. Cent. Sch.* **2015**, *3*, 1–20. [CrossRef]
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*, 1–20. [CrossRef]
6. Mirea, M.; Wang, V.; Jung, J. The not so dark side of the darknet: A qualitative study. *Secur. J.* **2019**, *32*, 102–118. [CrossRef]
7. Arabnezhad, E.; La Morgia, M.; Mei, A.; Nemmi, E.N.; Stefa, J. A Light in the Dark Web: Linking Dark Web Aliases to Real Internet Identities. In Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, 29 November–1 December 2020; pp. 311–321. [CrossRef]
8. Everett, C. Should the dark net be taken out? *Netw. Secur.* **2015**, *2015*, 10–13. [CrossRef]
9. Masson, K.; Bancroft, A. 'Nice people doing shady things': Drugs and the morality of exchange in the darknet cryptomarkets. *Int. J. Drug Policy* **2018**, *58*, 78–84. [CrossRef] [PubMed]
10. Jardine, E. Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies. *New Media Soc.* **2018**, *20*, 2824–2843. [CrossRef]
11. Biddle, P.; England, P.; Peinado, M.; Willman, B. The darknet and the future of content distribution. *ACM Workshop Digit. Rights Manag.* **2002**, *6*, 54.
12. Majam, T.; Theron, F. The purpose and relevance of a scientific literature review: A holistic approach to research. *J. Public Adm.* **2006**, *41*, 603–615.
13. Chen, H. *Dark Web Research Overview*; Springer: Berlin/Heidelberg, Germany, 2012; pp.3–18.
14. Dittus, M.; Wright, J.; Graham, M. Platform Criminalism: The 'Last-Mile' Geography of the Darknet Market Supply Chain. In Proceedings of the 2018 World Wide Web Conference, Lyon, France, 23–27 April 2018; pp. 277–286. [CrossRef]
15. Zhang, H.; Zou, F. A Survey of the Dark Web and Dark Market Research. In Proceedings of the 2020 IEEE 6th International Conference on Computer and Communications (ICCC), Chengdu, China, 11–14 December 2020; pp. 1694–1705. [CrossRef]
16. Pete, I.; Hughes, J.; Chua, Y.T.; Bada, M. A social network analysis and comparison of six dark web forums. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 16–18 June 2020; pp. 484–493.
17. Lusthaus, J. Beneath the Dark Web: Excavating the Layers of Cybercrime's Underground Economy. In Proceedings of the 2019 IEEE European symposium on security and privacy workshops (EuroS&PW), Stockholm, Sweden, 17–19 June 2019; pp. 474–480.

18. Ali, A.; Khan, M.; Saddique, M.; Pirzada, U.; Zohaib, M.; Ahmad, I.; Debnath, N. TOR vs I2P: A comparative study. In Proceedings of the 2016 IEEE International Conference on Industrial Technology (ICIT), Taipei, Taiwan, 14–17 March 2016; pp. 1748–1751. [CrossRef]
19. Hout, M.C.V.; Bingham, T. 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *Int. J. Drug Policy* **2013**, *24*, 385–391. [CrossRef]
20. Goecks, J.; Edwards, W.K.; Mynatt, E.D. Challenges in Supporting End-User Privacy and Security Management with Social Navigation. In Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain View, CA, USA, 15–17 July 2009. [CrossRef]
21. Chalhoub, G.; Flechais, I.; Nthala, N.; Abu-Salma, R.; Tom, E. Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. In Proceedings of the Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu HI USA 25–30 April 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–9. [CrossRef]
22. Liu, F.; Pan, L.; Yao, L. Evolutionary Game Based Analysis for User Privacy Protection Behaviors in Social Networks. In Proceedings of the 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 18–21 June 2018; pp. 274–279. [CrossRef]
23. Okoli, C.; Schabram, K. A Guide to Conducting a Systematic Literature Review of Information Systems Research. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1954824 (accessed on 30 March 2022).
24. Stowell, E.; Lyson, M.C.; Saksono, H.; Wurth, R.C.; Jimison, H.; Pavel, M.; Parker, A.G. Designing and evaluating mHealth interventions for vulnerable populations: A systematic review. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 21–26 April 2018; pp. 1–17.
25. Noah, N.; Das, S. Exploring evolution of augmented and virtual reality education space in 2020 through systematic literature review. *Comput. Animat. Virtual Worlds* **2021**, *32*, e2020. [CrossRef]
26. Nazah, S.; Huda, S.; Abawajy, J.; Hassan, M.M. Evolution of Dark Web threat analysis and detection: A systematic approach. *IEEE Access* **2020**, *8*, 171796–171819. [CrossRef]
27. Kolachala, K.; Simsek, E.; Ababneh, M.; Vishwanathan, R. SoK: Money Laundering in Cryptocurrencies. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; pp. 1–10.
28. Sánchez-Peralta, L.F.; Bote-Curiel, L.; Picón, A.; Sánchez-Margallo, F.M.; Pagador, J.B. Deep learning to find colorectal polyps in colonoscopy: A systematic literature review. *Artif. Intell. Med.* **2020**, 108, 101923. [CrossRef] [PubMed]
29. McInnes, M.D.; Moher, D.; Thombs, B.D.; McGrath, T.A.; Bossuyt, P.M.; Clifford, T.; Cohen, J.F.; Deeks, J.J.; Gatsonis, C.; Hooft, L.; et al. Preferred reporting items for a systematic review and meta-analysis of diagnostic test accuracy studies: The PRISMA-DTA statement. *JAMA* **2018**, *319*, 388–396. [CrossRef] [PubMed]
30. Moher, D.; Shamseer, L.; Clarke, M.; Ghersi, D.; Liberati, A.; Petticrew, M.; Shekelle, P.; Stewart, L.A. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Syst. Rev.* **2015**, *4*, 1. [CrossRef]
31. Ismailova, L.; Wolfengagen, V.; Kosikov, S. A Semantic Model for Indexing in the Hidden Web. *Procedia Comput. Sci.* **2021**, *190*, 324–331. [CrossRef]
32. Fang, Y.; Guo, Y.; Huang, C.; Liu, L. Analyzing and Identifying Data Breaches in Underground Forums. *IEEE Access* **2019**, *7*, 48770–48777. [CrossRef]
33. Jayswal, N. Attack Monitoring and Detection System using Dark IPs. *Int. J. Eng. Res. Technol.* **2014**, *3*, 1–5.
34. Schiller, B.; Roos, S.; Hofer, A.; Strufe, T. Attack Resistant Network Embeddings for Darknets. In Proceedings of the 2011 IEEE 30th Symposium on Reliable Distributed Systems Workshops, Washington, DC, USA, 4–7 October 2011; pp. 90–95. [CrossRef]
35. Bou-Harb, E.; Debbabi, M.; Assi, C. Behavioral analytics for inferring large-scale orchestrated probing events. In Proceedings of the 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 27 April–2 May 2014; pp. 506–511. [CrossRef]
36. Ding, J.; Guo, X.; Chen, Z. Big Data Analyses of ZeroNet Sites for Exploring the New Generation DarkWeb. In Proceedings of the 3rd International Conference on Software Engineering and Information Management, New York, NY, USA, 12–15 January 2020; pp. 46–52. [CrossRef]
37. Bou-Harb, E.; Husák, M.; Debbabi, M.; Assi, C. Big Data Sanitization and Cyber Situational Awareness: A Network Telescope Perspective. *IEEE Trans. Big Data* **2019**, *5*, 439–453. [CrossRef]
38. Fidalgo, E.; Alegre, E.; Fernández-Robles, L.; González-Castro, V. Classifying suspicious content in tor darknet through Semantic Attention Keypoint Filtering. *Digit. Investig.* **2019**, *30*, 12–22. [CrossRef]
39. Ríos, S.A.; Muñoz, R. Dark Web Portal Overlapping Community Detection Based on Topic Models. In Proceedings of the ACM SIGKDD Workshop on Intelligence and Security Informatics, Washington, DC, USA, 12 August 2012. [CrossRef]
40. Pourhabibi, T.; Ong, K.L.; Kam, B.H.; Boo, Y.L. DarkNetExplorer (DNE): Exploring dark multi-layer networks beyond the resolution limit. *Decis. Support Syst.* **2021**, *146*, 113537. [CrossRef]
41. Roos, S.; Strufe, T. Dealing with Dead Ends: Efficient Routing in Darknets. *ACM Trans. Model. Perform. Eval. Comput. Syst.* **2016**, *1*, 1–30. [CrossRef]
42. Mc Manamon, C.; Mtenzi, F. Defending privacy: The development and deployment of a darknet. In Proceedings of the 2010 International Conference for Internet Technology and Secured Transactions, London, UK, 8–10 December 2010; pp. 1–6.
43. Shestakov, D.; Bhowmick, S.S.; Lim, E.P. DEQUE: Querying the deep web. *Data Knowl. Eng.* **2005**, *52*, 273–311. [CrossRef]

44. Celestini, A.; Guarino, S. Design, Implementation and Test of a Flexible Tor-Oriented Web Mining Toolkit. In Proceedings of the 7th International Conference on Web Intelligence, Mining and Semantics, Amantea, Italy, 19–22 June 2017; Association for Computing Machinery: New York, NY, USA, 2017. [CrossRef]
45. Lawrence, H.; Hughes, A.; Tonic, R.; Zou, C. D-miner: A framework for mining, searching, visualizing, and alerting on darknet events. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017; pp. 1–9. [CrossRef]
46. Li, Z.; Alrwais, S.; Xie, Y.; Yu, F.; Wang, X. Finding the linchpins of the dark web: A study on topologically dedicated hosts on malicious web infrastructures. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 15–22 May 2013; pp. 112–126.
47. Yang, Y.; Yu, H.; Yang, L.; Yang, M.; Chen, L.; Zhu, G.; Wen, L. Hadoop-based Dark Web Threat Intelligence Analysis Framework. In Proceedings of the 2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, China, 25–27 May 2019; pp. 1088–1091.
48. Haga, Y.; Saso, A.; Mori, T.; Goto, S. Increasing the Darkness of Darknet Traffic. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–7. [CrossRef]
49. Li, K.; Liu, P.; Tan, Q.; Shi, J.; Gao, Y.; Wang, X. Out-of-Band Discovery and Evaluation for Tor Hidden Services. In Proceedings of the 31st Annual ACM Symposium on Applied Computing, Pisa, Italy, 4–8 April 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 2057–2062. [CrossRef]
50. Biswas, R.; González-Castro, V.; Fidalgo, E.; Alegre, E. Perceptual image hashing based on frequency dominant neighborhood structure applied to tor domains recognition. *Neurocomputing* **2020**, *383*, 24–38. [CrossRef]
51. Collier, B.; Stewart, J. Privacy Worlds: Exploring Values and Design in the Development of the Tor Anonymity Network. *Sci. Technol. Hum. Values* **2021**. [CrossRef]
52. Almukaynizi, M.; Nunes, E.; Dharaiya, K.; Senguttuvan, M.; Shakarian, J.; Shakarian, P. Proactive identification of exploits in the wild through vulnerability mentions online. In Proceedings of the 2017 International Conference on Cyber Conflict (CyCon U.S.), Washington, DC, USA, 7–8 November 2017; pp. 82–88. [CrossRef]
53. Mc Manamon, C.; Mtenzi, F. Proactive Privacy Protection with Darknets-The Development of Umbra. *Int. J. Inf. Secur. Res.* **2011**, *1*, 3–10. [CrossRef]
54. 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.
55. Khare, A.; Dalvi, A.; Kazi, F. Smart Crawler for Harvesting Deep web with Multi-Classification. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 1–3 July 2020; pp. 1–5. [CrossRef]
56. Schindler, S.; Schnor, B.; Scheffler, T. Taming the Ipv6 address space with hyhoneydv6. In Proceedings of the 2015 World Congress on Internet Security (WorldCIS), Dublin, Ireland, 19–21 October 2015; pp. 113–118. [CrossRef]
57. Owenson, G.; Cortes, S.; Lewman, A. The darknet's smaller than we thought: The life cycle of Tor Hidden Services. *Digit. Investig.* **2018**, *27*, 17–22. [CrossRef]
58. Al-Nabki, M.W.; Fidalgo, E.; Alegre, E.; Fernández-Robles, L. Torank: Identifying the most influential suspicious domains in the tor network. *Expert Syst. Appl.* **2019**, *123*, 212–226. [CrossRef]
59. Shoker, A. TorMass: Tor for the Masses Domestic and Monetized Anonymous Communication. *Procedia Comput. Sci.* **2021**, *181*, 1216–1224. [CrossRef]
60. Magán-Carrión, R.; Abellán-Galera, A.; Maciá-Fernández, G.; García-Teodoro, P. Unveiling the I2P web structure: A connectivity analysis. *Comput. Netw.* **2021**, *194*, 108158. [CrossRef]
61. Ebrahimi, M.; Samtani, S.; Chai, Y.; Chen, H. Detecting Cyber Threats in Non-English Hacker Forums: An Adversarial Cross-Lingual Knowledge Transfer Approach. In Proceedings of the 2020 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 21 May 2020; pp. 20–26. [CrossRef]
62. Bigham, J.P.; Cavender, A.C.; Kaminsky, R.S.; Prince, C.M.; Robison, T.S. Transcendence: Enabling a Personal View of the Deep Web. In Proceedings of the 13th International Conference on Intelligent User Interfaces, Gran Canaria, Spain, 13–16 January 2008; Association for Computing Machinery: New York, NY, USA, 2008; pp. 169–178. [CrossRef]
63. Ali, S.H.A.; Ozawa, S.; Ban, T.; Nakazato, J.; Shimamura, J. A neural network model for detecting DDoS attacks using darknet traffic features. In Proceedings of the 2016 International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, Canada, 24–29 July 2016; pp. 2979–2985. [CrossRef]
64. Zhang, Y.; Qian, Y.; Fan, Y.; Ye, Y.; Li, X.; Xiong, Q.; Shao, F. DStyle-GAN: Generative Adversarial Network Based on Writing and Photography Styles for Drug Identification in Darknet Markets. In Proceedings of the ACSAC '20 Annual Computer Security Applications Conference, Austin, TX, USA, 7–11 December 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 669–680. [CrossRef]
65. Roos, S.; Strufe, T. A contribution to analyzing and enhancing Darknet routing. In Proceedings of the 2013 Proceedings IEEE INFOCOM, Orlando, FL, USA, 25–30 March 2013; pp. 615–619. [CrossRef]

66. Popov, O.; Bergman, J.; Valassi, C. A Framework for a Forensically Sound Harvesting the Dark Web. In Proceedings of the Central European Cybersecurity Conference 2018, Ljubljana, Slovenia, 15–16 November 2018; Association for Computing Machinery: New York, NY, USA, 2018. [CrossRef]
67. Bou-Harb, E.; Debbabi, M.; Assi, C. A Time Series Approach for Inferring Orchestrated Probing Campaigns by Analyzing Darknet Traffic. In Proceedings of the 2015 10th International Conference on Availability, Reliability and Security, Washington, DC, USA, 24–27 August 2015; pp. 180–185. [CrossRef]
68. Spitters, M.; Verbruggen, S.; Van Staalduinen, M. Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services. In Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference, The Hague, The Netherlands, 24–26 September 2014; pp. 220–223. [CrossRef]
69. Moubarak, J.; Bassil, C. On Darknet HoneyBots. In Proceedings of the 2020 4th Cyber Security in Networking Conference (CSNet), Lausanne, Switzerland, 21–23 October 2020; pp. 1–3. [CrossRef]
70. Samtani, S.; Zhu, H.; Chen, H. Proactively Identifying Emerging Hacker Threats from the Dark Web: A Diachronic Graph Embedding Framework (D-GEF). *ACM Trans. Priv. Secur.* **2020**, *23*, 1–33. [CrossRef]
71. Tang, X.; Yang, C.C.; Zhang, M. Who Will Be Participating next? Predicting the Participation of Dark Web Community. In Proceedings of the ACM SIGKDD Workshop on Intelligence and Security Informatics, Beijing, China, 12 August 2012; Association for Computing Machinery: New York, NY, USA, 2012. [CrossRef]
72. Thomaz, F.; Salge, C.; Karahanna, E.; Hulland, J. Learning from the Dark Web: Leveraging conversational agents in the era of hyper-privacy to enhance marketing. *J. Acad. Mark. Sci.* **2020**, *48*, 43–63. [CrossRef]
73. Tai, X.H.; Soska, K.; Christin, N. Adversarial Matching of Dark Net Market Vendor Accounts. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, Anchorage, AK, USA, 4–8 August 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 1871–1880. [CrossRef]
74. Yannikos, Y.; Heeger, J.; Brockmeyer, M. An Analysis Framework for Product Prices and Supplies in Darknet Marketplaces. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; Association for Computing Machinery: New York, NY, USA, 2019. [CrossRef]
75. Al-Ramahi, M.; Alsmadi, I.; Davenport, J. Exploring Hackers Assets: Topics of Interest as Indicators of Compromise. In Proceedings of the 7th Symposium on Hot Topics in the Science of Security, Lawrence, KS, USA, 21–23 September 2020; Association for Computing Machinery: New York, NY, USA, 2020. [CrossRef]
76. Almukaynizi, M.; Marin, E.; Nunes, E.; Shakarian, P.; Simari, G.I.; Kapoor, D.; Siedlecki, T. DARKMENTION: A Deployed System to Predict Enterprise-Targeted External Cyberattacks. In Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Antonio, TX, USA, 2–3 November 2018; pp. 31–36. [CrossRef]
77. Kumar, S.; Vranken, H.; van Dijk, J.; Hamalainen, T. Deep in the Dark: A Novel Threat Detection System using Darknet Traffic. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 4273–4279.
78. Inoue, D.; Eto, M.; Suzuki, K.; Suzuki, M.; Nakao, K. DAEDALUS-VIZ: Novel Real-Time 3D Visualization for Darknet Monitoring-Based Alert System. In Proceedings of the Ninth International Symposium on Visualization for Cyber Security, Seattle, Wa, USA, 15 October 2012; Association for Computing Machinery: New York, NY, USA, 2012; pp. 72–79. [CrossRef]
79. Bailey, M.; Cooke, E.; Jahanian, F.; Myrick, A.; Sinha, S. Practical Darknet Measurement. In Proceedings of the 2006 40th Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, 22–24 March 2006; pp. 1496–1501. [CrossRef]
80. Hashimoto, N.; Ozawa, S.; Ban, T.; Nakazato, J.; Shimamura, J. A darknet traffic analysis for IoT malwares using association rule learning. *Procedia Comput. Sci.* **2018**, *144*, 118–123. [CrossRef]
81. Montieri, A.; Ciuonzo, D.; Bovenzi, G.; Persico, V.; Pescapé, A. A dive into the dark web: Hierarchical traffic classification of anonymity tools. *IEEE Trans. Netw. Sci. Eng.* **2019**, *7*, 1043–1054. [CrossRef]
82. Bou-Harb, E. A probabilistic model to preprocess darknet data for cyber threat intelligence generation. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6. [CrossRef]
83. Narita, M.; Kamada, K.; Ogura, K.; Bista, B.B.; Takata, T. A Study of Packet Sampling Methods for Protecting Sensors Deployed on Darknet. In Proceedings of the 2016 19th International Conference on Network-Based Information Systems (NBiS), Ostrava, Czech Republic, 7–9 September 2016; pp. 76–83. [CrossRef]
84. Furumoto, K.; Kashiki, K.; Morii, M.; Ikegami, M.; Hasegawa, T.; Ishikawa, T.; Nakao, K. Analysis of Multiple Darknet Focusing on Outbound Packets and its Application to Malware Analysis. In Proceedings of the 2017 Fifth International Symposium on Computing and Networking (CANDAR), Aomori, Japan, 19–22 November 2017; pp. 94–100. [CrossRef]
85. Vichaidis, N.; Tsunoda, H.; Keeni, G.M. Analyzing darknet TCP traffic stability at different timescales. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 128–133.
86. Montieri, A.; Ciuonzo, D.; Aceto, G.; Pescapé, A. Anonymity services tor, i2p, jondonym: Classifying in the dark (web). *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 662–675. [CrossRef]
87. Soro, F.; Drago, I.; Trevisan, M.; Mellia, M.; Ceron, J.; Santanna, J. Are Darknets All The Same? On Darknet Visibility for Security Monitoring. In Proceedings of the 2019 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), Paris, France, 1–3 July 2019; pp. 1–6. [CrossRef]

88. Evrard, L.; François, J.; Colin, J.N. Attacker Behavior-Based Metric for Security Monitoring Applied to Darknet Analysis. In Proceedings of the 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Washington DC, USA, 8–12 April 2019; pp. 89–97.
89. Burda, P.; Boot, C.; Allodi, L. Characterizing the Redundancy of DarkWeb Onion Services. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; Association for Computing Machinery: New York, NY, USA, 2019. [CrossRef]
90. Gadhia, F.; Choi, J.; Cho, B.; Song, J. Comparative analysis of darknet traffic characteristics between darknet sensors. In Proceedings of the 2015 17th International Conference on Advanced Communication Technology (ICACT), Seoul, Korea, 1–3 July 2015; pp. 59–64. [CrossRef]
91. Yang, Y.; Zhu, G.; Yang, L.; Yu, H. Crawling and Analysis of Dark Network Data. In Proceedings of 2020 the 6th International Conference on Computing and Data Engineering, Sanya, China, 4–6 January 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 116–120. [CrossRef]
92. Fachkha, C. Cyber Threat Investigation of SCADA Modbus Activities. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019; pp. 1–7. [CrossRef]
93. Ma, H.; Cao, J.; Mi, B.; Huang, D.; Liu, Y.; Zhang, Z. Dark web traffic detection method based on deep learning. In Proceedings of the 2021 IEEE 10th Data Driven Control and Learning Systems Conference (DDCLS), Suzhou, China, 14–16 May 2021; pp. 842–847.
94. Mizoguchi, S.; Fukushima, Y.; Kasahara, Y.; Hori, Y.; Sakurai, K. Darknet Monitoring on Real-Operated Networks. In Proceedings of the 2010 International Conference on Broadband, Wireless Computing, Communication and Applications, Fukuoka, Japan, 4–6 November 2010; pp. 278–285. [CrossRef]
95. Iliadis, L.A.; Kaifas, T. Darknet Traffic Classification using Machine Learning Techniques. In Proceedings of the 2021 10th International Conference on Modern Circuits and Systems Technologies (MOCAST), Stockholm, Vienna, 5–7 July 2021; pp. 1–4. [CrossRef]
96. Steinebach, M.; Schäfer, M.; Karakuz, A.; Brandl, K. Detection and Analysis of Tor Onion Services. *J. Cyber Secur. Mobil.* **2019**, *9*, 1–10.
97. Škrjanc, I.; Ozawa, S.; Dovžan, D.; Tao, B.; Nakazato, J.; Shimamura, J. Evolving cauchy possibilistic clustering and its application to large-scale cyberattack monitoring. In Proceedings of the 2017 IEEE Symposium Series on Computational Intelligence (SSCI), Honolulu, HA, USA, 27 November–1 December 2017; pp. 1–7. [CrossRef]
98. Höfer, A.; Roos, S.; Strufe, T. Greedy Embedding, Routing and Content Addressing for Darknets. In Proceedings of the 2013 Conference on Networked Systems, Madrid, Spain, 2–5 April 2013; pp. 43–50. [CrossRef]
99. Pour, M.S.; Bou-Harb, E. Implications of Theoretic Derivations on Empirical Passive Measurements for Effective Cyber Threat Intelligence Generation. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–7. [CrossRef]
100. Park, J.; Mun, H.; Lee, Y. Improving Tor Hidden Service Crawler Performance. In Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, 10–13 December 2018; pp. 1–8. [CrossRef]
101. De Santis, G.; Lahmadi, A.; Francois, J.; Festor, O. Internet-Wide Scanners Classification using Gaussian Mixture and Hidden Markov Models. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5. [CrossRef]
102. Fachkha, C.; Bou-Harb, E.; Boukhtouta, A.; Dinh, S.; Iqbal, F.; Debbabi, M. Investigating the dark cyberspace: Profiling, threat-based analysis and correlation. In Proceedings of the 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), Cork, Ireland, 10–12 October 2012; pp. 1–8. [CrossRef]
103. Lagraa, S.; François, J. Knowledge discovery of port scans from darknet. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 935–940. [CrossRef]
104. Nishikaze, H.; Ozawa, S.; Kitazono, J.; Ban, T.; Nakazato, J.; Shimamura, J. Large-scale monitoring for cyber attacks by using cluster information on darknet traffic features. *Procedia Comput. Sci.* **2015**, *53*, 175–182. [CrossRef]
105. Akshobhya, K. Machine learning for anonymous traffic detection and classification. In Proceedings of the 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, Uttar Pradesh, 28–29 January 2021; pp. 942–947.
106. De Santis, G.; Lahmadi, A.; Francois, J.; Festor, O. Modeling of IP Scanning Activities with Hidden Markov Models: Darknet Case Study. In Proceedings of the 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Larnaca, Cyprus, 21–23 November 2016; pp. 1–5. [CrossRef]
107. Woodhead, S. Monitoring bad traffic with darknets. *Netw. Secur.* **2012**, *2012*, 10–14. [CrossRef]
108. AlShehyari, S.; Yeun, C.Y.; Damiani, E. Monitoring darknet activities by using network telescope. In Proceedings of the 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 11–14 December 2017; pp. 123–128. [CrossRef]
109. Balkanli, E.; Zincir-Heywood, A.N. On the analysis of backscatter traffic. In Proceedings of the 39th Annual IEEE Conference on Local Computer Networks Workshops, Edmonton, AB, Canada, 8–11 September 2014; pp. 671–678. [CrossRef]
110. Roos, S.; Strufe, T. Provable Polylog Routing for Darknets. In Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops, Washington, DC, USA, 8–21 June 2012; pp. 140–146. [CrossRef]

111. Soro, F.; Allegretta, M.; Mellia, M.; Drago, I.; Bertholdo, L.M. Sensing the Noise: Uncovering Communities in Darknet Traffic. In Proceedings of the 2020 Mediterranean Communication and Computer Networking Conference (MedComNet), Arona, Italy, 17–19 June 2020; pp. 1–8. [CrossRef]
112. Wang, P.; Liu, H.; Wang, B.; Dong, K.; Wang, L.; Xu, S. Simulation of Dark Network Scene Based on the Big Data Environment. In Proceedings of the International Conference on Information Technology and Electrical Engineering 2018, Xiamen, China, 7–8 December 2018; Association for Computing Machinery: New York, NY, USA, 2018. [CrossRef]
113. Joshi, P.S.; Dinesha, H. Survey on Identification of Malicious Activities by Monitoring Darknet Access. In Proceedings of the 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 August 2020; pp. 346–350. [CrossRef]
114. Xu, J.; Chen, H. The Topology of Dark Networks. *Commun. ACM* **2008**, *51*, 58–65. [CrossRef]
115. Pour, M.S.; Bou-Harb, E. Theoretic derivations of scan detection operating on darknet traffic. *Comput. Commun.* **2019**, *147*, 111–121. [CrossRef]
116. Cabana, O.; Youssef, A.M.; Debbabi, M.; Lebel, B.; Kassouf, M.; Atallah, R.; Agba, B.L. Threat Intelligence Generation Using Network Telescope Data for Industrial Control Systems. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3355–3370. [CrossRef]
117. Coudriau, M.; Lahmadi, A.; François, J. Topological analysis and visualisation of network monitoring data: Darknet case study. In Proceedings of the 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, United Arab Emirates, 4–7 December 2016; pp. 1–6. [CrossRef]
118. Liu, J.; Fukuda, K. Towards a taxonomy of darknet traffic. In Proceedings of the 2014 International Wireless Communications and Mobile Computing Conference (IWCMC), Nicosia, Cyprus, 4–8 August 2014; pp. 37–43. [CrossRef]
119. Hu, Y.; Zou, F.; Li, L.; Yi, P. Traffic Classification of User Behaviors in Tor, I2P, ZeroNet, Freenet. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 10–13 November 2020; pp. 418–424. [CrossRef]
120. Vichaidis, N.; Tsunoda, H. Using normalized entropy to compare traffic differences in stable and unstable time slots. In Proceedings of the 2018 5th International Conference on Business and Industrial Research (ICBIR), Bangkok, Thailand, 17–18 May 2018; pp. 21–24. [CrossRef]
121. Atifi, A.; Bou-Harb, E. On correlating network traffic for cyber threat intelligence: A Bloom filter approach. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 384–389. [CrossRef]
122. Hoang, N.P.; Kintis, P.; Antonakakis, M.; Polychronakis, M. An Empirical Study of the I2P Anonymity Network and Its Censorship Resistance. In Proceedings of the Internet Measurement Conference 2018, Boston, MA, USA, 31 October–2 November 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 379–392. [CrossRef]
123. Platzer, F.; Schäfer, M.; Steinebach, M. Critical Traffic Analysis on the Tor Network. *J. Cyber Secur. Mobil.* **2021**, *10*, 1–10. [CrossRef]
124. Jardine, E. Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New Media Soc.* **2018**, *20*, 435–452. [CrossRef]
125. Akiyoshi, R.; Kotani, D.; Okabe, Y. Detecting Emerging Large-Scale Vulnerability Scanning Activities by Correlating Low-Interaction Honeypots with Darknet. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018; Volume 2, pp. 658–663. [CrossRef]
126. Yoshioka, K.; Matsumoto, T. Fingerprinting Traffic Log. In Proceedings of the 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Washington, DC, USA, 15–17 August 2008; pp. 143–146. [CrossRef]
127. Wang, Q.; Chen, Z.; Chen, C. Darknet-Based Inference of Internet Worm Temporal Characteristics. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 1382–1393. [CrossRef]
128. Catakoglu, O.; Balduzzi, M.; Balzarotti, D. Attacks Landscape in the Dark Side of the Web. In Proceedings of the Symposium on Applied Computing, Marrakech, Morocco, 3–7 April 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 1739–1746. [CrossRef]
129. Matic, S.; Kotzias, P.; Caballero, J. CARONTE: Detecting Location Leaks for Deanonymizing Tor Hidden Services. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; Association for Computing Machinery: New York, NY, USA, 2015; pp. 1455–1466. [CrossRef]
130. Cambiaso, E.; Vaccari, I.; Patti, L.; Aiello, M. *Darknet Security: A Categorization of Attacks to the Tor Network*; ITASEC: Rome, Italy, 2019; pp.1–12.
131. Furutani, N.; Ban, T.; Nakazato, J.; Shimamura, J.; Kitazono, J.; Ozawa, S. Detection of DDoS Backscatter Based on Traffic Features of Darknet TCP Packets. In Proceedings of the 2014 Ninth Asia Joint Conference on Information Security, Wuhan, China, 3–5 September 2014; pp. 39–43. [CrossRef]
132. Habibi Lashkari, A.; Kaur, G.; Rahali, A. DIDarknet: A Contemporary Approach to Detect and Characterize the Darknet Traffic Using Deep Image Learning. In Proceedings of the 10th International Conference on Communication and Network Security, Tokyo, Japan, 27–29 November 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–13. [CrossRef]
133. Yoon, C.; Kim, K.; Kim, Y.; Shin, S.; Son, S. DoppelgäNgers on the Dark Web: A Large-Scale Assessment on Phishing Hidden Web Services. In Proceedings of the The World Wide Web Conference, San Francisco, CA, USA, 13-17 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 2225–2235. [CrossRef]

134. Almukaynizi, M.; Paliath, V.; Shah, M.; Shah, M.; Shakarian, P. Finding Cryptocurrency Attack Indicators Using Temporal Logic and Darkweb Data. In Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), San Antonio, TX, USA, 2–3 November 2018; pp. 91–93. [CrossRef]
135. Fachkha, C.; Bou-Harb, E.; Debbabi, M. Fingerprinting Internet DNS Amplification DDoS Activities. In Proceedings of the 2014 6th International Conference on New Technologies, Mobility and Security (NTMS), Dubai, United Arab Emirates, 30 March–2 April 2014; pp. 1–5. [CrossRef]
136. Fachkha, C.; Bou-Harb, E.; Debbabi, M. Inferring distributed reflection denial of service attacks from darknet. *Comput. Commun.* **2015**, *62*, 59–71. [CrossRef]
137. Wang, Q.; Chen, Z.; Makki, K.; Pissinou, N.; Chen, C. Inferring Internet Worm Temporal Characteristics. In Proceedings of the IEEE GLOBECOM 2008—2008 IEEE Global Telecommunications Conference, New Orleans, Louisiana, 30 November–4 December 2008; pp. 1–6. [CrossRef]
138. Bou-Harb, E.; Fachkha, C.; Debbabi, M.; Assi, C. Inferring internet-scale infections by correlating malware and probing activities. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 10–14 June 2014; pp. 640–646. [CrossRef]
139. Zeid, R.B.; Moubarak, J.; Bassil, C. Investigating The Darknet. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 727–732. [CrossRef]
140. Barr-Smith, F.; Wright, J. Phishing With A Darknet: Imitation of Onion Services. In Proceedings of the 2020 APWG Symposium on Electronic Crime Research (eCrime), Virtual, 16–19 November 2020; pp. 1–13. [CrossRef]
141. Han, C.; Shimamura, J.; Takahashi, T.; Inoue, D.; Kawakita, M.; Takeuchi, J.; Nakao, K. Real-Time Detection of Malware Activities by Analyzing Darknet Traffic Using Graphical Lasso. In Proceedings of the 2019 18th IEEE International Conference On Trust, Security and Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019; pp. 144–151. [CrossRef]
142. Meland, P.H.; Bayoumy, Y.F.F.; Sindre, G. The Ransomware-as-a-Service economy within the darknet. *Comput. Secur.* **2020**, *92*, 101762. [CrossRef]
143. Ban, T.; Pang, S.; Eto, M.; Inoue, D.; Nakao, K.; Huang, R. Towards Early Detection of Novel Attack Patterns through the Lens of a Large-Scale Darknet. In Proceedings of the 2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Toulouse, France, 18–21 July 2016. [CrossRef]
144. Shen, S.; Gao, J.; Wu, A. Weakness Identification and Flow Analysis Based on Tor Network. In Proceedings of the 8th International Conference on Communication and Network Security, Qingdao, China, 2–4 November 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 90–94. [CrossRef]
145. Negri, A.; Townshend, H.; McSweeney, T.; Angelopoulou, O.; Banayoti, H.; Prilutskaya, M.; Bowden-Jones, O.; Corazza, O. Carfentanil on the darknet: Potential scam or alarming public health threat? *Int. J. Drug Policy* **2021**, *91*, 103118. [CrossRef] [PubMed]
146. 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]
147. Brenner, F.; Platzer, F.; Steinebach, M. Discovery of Single-Vendor Marketplace Operators in the Tor-Network. In Proceedings of 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; Association for Computing Machinery: New York, NY, USA, 2021. [CrossRef]
148. Kumar, R.; Yadav, S.; Daniulaityte, R.; Lamy, F.; Thirunarayan, K.; Lokala, U.; Sheth, A. EDarkFind: Unsupervised Multi-View Learning for Sybil Account Detection. In Proceedings of The Web Conference 2020, Taipei, Taiwan, 20–24 April 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1955–1965.
149. Phelps, A.; Watt, A. I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digit. Investig.* **2014**, *11*, 261–272. [CrossRef]
150. Kanemura, K.; Toyoda, K.; Ohtsuki, T. Identification of Darknet Markets' Bitcoin Addresses by Voting Per-address Classification Results. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 15–17 May 2019; pp. 154–158. [CrossRef]
151. 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. [CrossRef]
152. Lane, B.R.; Salmon, P.M.; Desmond, D.; Cherney, A.; Carley, A.; Hulme, A.; Stanton, N.A. Out of control? Using STAMP to model the control and feedback mechanisms surrounding identity crime in darknet marketplaces. *Appl. Ergon.* **2020**, *89*, 103223. [CrossRef]
153. Adewopo, V.; Gonen, B.; Varlioglu, S.; Ozer, M. Plunge into the Underworld: A Survey on Emergence of Darknet. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 5–7 December 2019; pp. 155–159. [CrossRef]
154. Marin, E.; Diab, A.; Shakarian, P. Product offerings in malicious hacker markets. In Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28 September–1 October 2016; pp. 187–189. [CrossRef]
155. Espinosa, R. Scamming and the reputation of drug dealers on Darknet Markets. *Int. J. Ind. Organ.* **2019**, *67*, 102523. [CrossRef]

156. Krstenic, A. The Dark Net as a New Black Market and Security Issue. Available online: https://rabek.org/en/wp-content/uploads/sites/3/2017/10/ZBORNIK-ENG.pdf#page=22 (accessed on 30 March 2022).
157. Thomaz, F. The digital and physical footprint of dark net markets. *J. Int. Mark.* **2020**, *28*, 66–80. [CrossRef]
158. Chaudhry, P.E. The looming shadow of illicit trade on the internet. *Bus. Horizons* **2017**, *60*, 77–89. [CrossRef]
159. Jeziorowski, S.; Ismail, M.; Siraj, A. Towards Image-Based Dark Vendor Profiling: An Analysis of Image Metadata and Image Hashing in Dark Web Marketplaces. In Proceedings of the Sixth International Workshop on Security and Privacy Analytics, New Orleans, LA, USA, 18 March 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 15–22. [CrossRef]
160. Trautman, L. Virtual currencies: Bitcoin & what now after liberty reserve, silk road, and mt. gox. *Rich. Tech.* **2013**, *20*, 1.
161. Wang, X.; Peng, P.; Wang, C.; Wang, G. You Are Your Photographs: Detecting Multiple Identities of Vendors in the Darknet Marketplaces. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security, Incheon, Korea, 4 June 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 431–442. [CrossRef]
162. Zhang, Y.; Fan, Y.; Song, W.; Hou, S.; Ye, Y.; Li, X.; Zhao, L.; Shi, C.; Wang, J.; Xiong, Q. Your Style Your Identity: Leveraging Writing and Photography Styles for Drug Trafficker Identification in Darknet Markets over Attributed Heterogeneous Information Network. In Proceedings of the World Wide Web Conference, San Francisco, CA, USA, 13-17 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 3448–3454. [CrossRef]
163. Zabihimayvan, M.; Sadeghi, R.; Doran, D.; Allahyari, M. A Broad Evaluation of the Tor English Content Ecosystem. In Proceedings of the 10th ACM Conference on Web Science, Boston, MA, USA, 30 June–3 July 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 333–342. [CrossRef]
164. Guitton, C. A review of the available content on Tor hidden services: The case against further development. *Comput. Hum. Behav.* **2013**, *29*, 2805–2815. [CrossRef]
165. 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]
166. Beshiri, A.S.; Susuri, A. Dark web and its impact in online anonymity and privacy: A critical analysis and review. *J. Comput. Commun.* **2019**, *7*, 30. [CrossRef]
167. Kaur, S.; Randhawa, S. Dark Web: A Web of Crimes. *Wirel. Pers. Commun.* **2020**, *112*, 2131–2158. [CrossRef]
168. Han, W.; Duong, V.; Nguyen, L.; Mier, C. Darknet and Bitcoin De-anonymization: Emerging Development. In Proceedings of the 2020 Zooming Innovation in Consumer Technologies Conference (ZINC), Novi Sad, Serbia, 26–27 May 2020; pp. 222–226. [CrossRef]
169. Fachkha, C.; Debbabi, M. Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 1197–1227. [CrossRef]
170. Mansfield-Devine, S. Darknets. *Comput. Fraud. Secur.* **2009**, *2009*, 4–6. [CrossRef]
171. Ranakoti, P.; Yadav, S.; Apurva, A.; Tomer, S.; Roy, N.R. Deep web amp; online anonymity. In Proceedings of the 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), Gurgaon, India, 12–14 October 2017; pp. 215–219. [CrossRef]
172. El-Gamil, B.R.; Winiwarter, W.; Božić, B.; Wahl, H. Deep Web Integrated Systems: Current Achievements and Open Issues. In Proceedings of the 13th International Conference on Information Integration and Web-Based Applications and Services, Ho Chi Minh City, Vietnam, 5–7 December 2011; Association for Computing Machinery: New York, NY, USA, 2011; pp. 447–450. [CrossRef]
173. Hatta, M. Deep web, dark web, dark net A taxonomy of "hidden" Internet. *Ann. Bus. Adm. Sci.* **2020**, *7*, 0200908a.
174. Bernaschi, M.; Celestini, A.; Guarino, S.; Lombardi, F. Exploring and Analyzing the Tor Hidden Services Graph. *ACM Trans. Web* **2017**, *11*, 3008662. [CrossRef]
175. Bellaby, R.W. Going dark: Anonymising technology in cyberspace. *Ethics Inf. Technol.* **2018**, *20*, 189–204. [CrossRef]
176. Tapia, M.G.; Shorter, J. Into the depths of the internet: The deep web. *Issues Inf. Syst.* **2015**, *16*, 3. [CrossRef]
177. Hoeller, T.; Roland, M.; Mayrhofer, R. On the State of V3 Onion Services. In Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet, Virtual Event, 27 August 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 50–56. [CrossRef]
178. Ban, T.; Inoue, D. Practical darknet traffic analysis: Methods and case studies. In Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computed, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, USA, 4–8 August 2017; pp. 1–8. [CrossRef]
179. Bernaschi, M.; Celestini, A.; Guarino, S.; Lombardi, F.; Mastrostefano, E. Spiders like Onions: On the Network of Tor Hidden Services. In Proceedings of the World Wide Web Conference, San Francisco, CA, USA, 13–17 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 105–115. [CrossRef]
180. Broadhead, S. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Comput. Law Secur. Rev.* **2018**, *34*, 1180–1196. [CrossRef]
181. Bhushan, B.; Saxena, S. The Dark Web: A Dive Into the Darkest Side of the Internet. Available online https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598902 (accessed on 30 March 2022).

182. Sanchez-Rola, I.; Balzarotti, D.; Santos, I. The Onions Have Eyes: A Comprehensive Structure and Privacy Analysis of Tor Hidden Services. In Proceedings of the 26th International Conference on World Wide Web, Perth, Australia, 3–7 April 2017; Conferences Steering Committee: Republic and Canton of Geneva, Switzerland, 2017; pp. 1251–1260. [CrossRef]
183. He, S.; He, Y.; Li, M. Classification of Illegal Activities on the Dark Web. In Proceedings of the 2019 2nd International Conference on Information Science and Systems, Tokyo, Japan, 16–19 March 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 73–78. [CrossRef]
184. Bancroft, A.; Reid, P.S. Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. *Int. J. Drug Policy* **2016**, *35*, 42–49. [CrossRef] [PubMed]
185. 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]
186. Vana, P.; Pachigolla, P. *Do Law Enforcement Busts of Darknet Markets Deter Criminal Activity in Other Darknet Markets?* SSRN: Amsterdam, The Netherlands, 2019.
187. Witting, S.K. Do Ut Des: Disseminating Online Child Sexual Abuse Material for Investigative Purposes? In Proceedings of the Central European Cybersecurity Conference 2018, Ljubljana, Slovenia, 15–16 November 2018; Association for Computing Machinery: New York, NY, USA, 2018. [CrossRef]
188. 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]
189. Iliou, C.; Kalpakis, G.; Tsikrika, T.; Vrochidis, S.; Kompatsiaris, I. Hybrid Focused Crawling for Homemade Explosives Discovery on Surface and Dark Web. In Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2016; pp. 229–234. [CrossRef]
190. Akyıldız, O. Information analysis and cyber crimes in Deep Web amp; Dark Web. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–6. [CrossRef]
191. Kokolaki, E.; Daskalaki, E.; Psaroudaki, K.; Christodoulaki, M.; Fragopoulou, P. Investigating the dynamics of illegal online activity: The power of reporting, dark web, and related legislation. *Comput. Law Secur. Rev.* **2020**, *38*, 105440. [CrossRef]
192. Pantelis, G.; Petrou, P.; Karagiorgou, S.; Alexandrou, D. On Strengthening SMEs and MEs Threat Intelligence and Awareness by Identifying Data Breaches, Stolen Credentials and Illegal Activities on the Dark Web. In Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; Association for Computing Machinery: New York, NY, USA, 2021. [CrossRef]
193. Van Hout, M.C.; Bingham, T. Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *Int. J. Drug Policy* **2014**, *25*, 183–189. [CrossRef]
194. Bradley, C.; Stringhini, G. A qualitative evaluation of two different law enforcement approaches on dark net markets. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, 17–19 June 2019; pp. 453–463.
195. Yang, C.C.; Tang, X.; Thuraisingham, B.M. An Analysis of User Influence Ranking Algorithms on Dark Web Forums. In Proceedings of the ACM SIGKDD Workshop on Intelligence and Security Informatics, Washington, DC, USA, 25–28 July 2010; Association for Computing Machinery: New York, NY, USA, 2010. [CrossRef]
196. Kamphausen, G.; Werse, B. Digital figurations in the online trade of illicit drugs: A qualitative content analysis of darknet forums. *Int. J. Drug Policy* **2019**, *73*, 281–287. [CrossRef]
197. Adewopo, V.; Gonen, B.; Adewopo, F. Exploring Open Source Information for Cyber Threat Intelligence. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 10–13 December 2020; pp. 2232–2241. [CrossRef]
198. Bazanov, V.V.; Frolov, A.A.; Arzhskov, A.V. Method for Identifying Dangerous Forum Posts on the Onion Network. In Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, 27–30 January 2020; pp. 229–232. [CrossRef]
199. Almukaynizi, M.; Grimm, A.; Nunes, E.; Shakarian, J.; Shakarian, P. Predicting Cyber Threats through Hacker Social Networks in Darkweb and Deepweb Forums. In Proceedings of the 2017 International Conference of The Computational Social Science Society of the Americas, Santa Fe, NM, USA, 19–22 October 2017; Association for Computing Machinery: New York, NY, USA, 2017. [CrossRef]
200. Park, A.J.; Beck, B.; Fletche, D.; Lam, P.; Tsang, H.H. Temporal Analysis of Radical Dark Web Forum Users. In Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, San Francisco, CA, USA, 18–21 August 2016; pp. 880–883.
201. Mörch, C.M.; Cote, L.P.; Corthesy-Blondin, L.; Plourde-Léveillé, L.; Dargis, L.; Mishara, B.L. The Darknet and suicide. *J. Affect. Disord.* **2018**, *241*, 127–132. [CrossRef]
202. L'Huillier, G.; Ríos, S.A.; Alvarez, H.; Aguilera, F. Topic-Based Social Network Analysis for Virtual Communities of Interests in the Dark Web. In Proceedings of the ACM SIGKDD Workshop on Intelligence and Security Informatics, Washington, DC, USA, 25–28 July 2010; Association for Computing Machinery: New York, NY, USA, 2010. [CrossRef]
203. Sun, Z.; Rubio-Medrano, C.E.; Zhao, Z.; Bao, T.; Doupé, A.; Ahn, G.J. Understanding and Predicting Private Interactions in Underground Forums. In Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy, Richardson, TX, USA, 25–27 March 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 303–314. [CrossRef]

204. Sennewald, B.; Herpers, R.; Hülsmann, M.; Kent, K.B. Voting for Authorship Attribution Applied to Dark Web Data. In Proceedings of the 30th Annual International Conference on Computer Science and Software Engineering, Hiroshima, Japan, 26–30 March 2020; pp. 217–226.
205. Van Hout, M.C.; Bingham, T. 'Surfing the Silk Road': A study of users' experiences. *Int. J. Drug Policy* **2013**, *24*, 524–529. [CrossRef]
206. Lazarenko, A.; Avdoshin, S. Anonymity of Tor: Myth and Reality. In Proceedings of the 12th Central and Eastern European Software Engineering Conference in Russia, Moscow, Russia, 28–29 October 2016; Association for Computing Machinery: New York, NY, USA, 2016. [CrossRef]
207. Liu, Y.; Lin, F.Y.; Ahmad-Post, Z.; Ebrahimi, M.; Zhang, N.; Hu, J.L.; Xin, J.; Li, W.; Chen, H. Identifying, collecting, and monitoring personally identifiable information: From the dark web to the surface web. In Proceedings of the 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Arlington, VA, USA, 9–10 November 2020; pp. 1–6.
208. Lin, F.; Liu, Y.; Ebrahimi, M.; Ahmad-Post, Z.; Hu, J.L.; Xin, J.; Samtani, S.; Li, W.; Chen, H. Linking personally identifiable information from the dark web to the surface web: A deep entity resolution approach. In Proceedings of the 2020 International Conference on Data Mining Workshops (ICDMW), Sorrento, Italy, 17–20 November 2020; pp. 488–495.
209. Tavabi, N.; Bartley, N.; Abeliuk, A.; Soni, S.; Ferrara, E.; Lerman, K. Characterizing Activity on the Deep and Dark Web. In 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.
210. Al Jawaheri, H.; Al Sabah, M.; Boshmaf, Y.; Erbad, A. Deanonymizing Tor hidden service users through Bitcoin transactions analysis. *Comput. Secur.* **2020**, *89*, 101684. [CrossRef]
211. La Morgia, M.; Mei, A.; Raponi, S.; Stefa, J. Time-zone geolocation of crowds in the dark web. In Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, 2–6 July 2018; pp. 445–455.
212. Mihelič, A.; Markelj, B.; Bernik, I.; Zgaga, S. Investigating the Darknet: Limitations in Slovenian Legal System. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–1 September 2017; Association for Computing Machinery: New York, NY, USA, 2017. [CrossRef]
213. Chan, J.; He, S.; Qiao, D.; Whinston, A.B. *Shedding Light on the Dark: The Impact of Legal Enforcement on Darknet Transactions*; NET Institute Working Paper No. 19-08; NET Institute: Amsterdam, The Netherlands, 2019; SSRN 3468426.
214. Minárik, T.; Osula, A.M. Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law. *Comput. Law Secur. Rev.* **2016**, *32*, 111–127. [CrossRef]
215. Ahmad, W.; Liccardi, I. Addressing Anonymous Abuses: Measuring the Effects of Technical Mechanisms on Reported User Behaviors. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 25 April 2020; pp. 1–14.
216. Huang, H.Y.; Bashir, M. The Onion Router: Understanding a Privacy Enhancing Technology Community. *Proc. Assoc. Inf. Sci. Technol.* **2016**, *53*, 1–10. [CrossRef]
217. Odendaal, R.; Hattingh, M.; Eybers, S. The Good, the Bad and the Ugly of the Dark Web: Perceptions of South African Students and Parents. In Proceedings of the South African Institute of Computer Scientists and Information Technologists 2019, Skukuza, South Africa, 17–18 September 2019; Association for Computing Machinery: New York, NY, USA, 2019. [CrossRef]
218. Jardine, E. Online content moderation and the dark web: Policy responses to radicalizing hate speech and malicious content on the darknet. *First Monday* **2019**, 4, 12. [CrossRef]
219. Sherer, J.A.; McLellan, M.L.; Fedeles, E.R.; Sterling, N.L. Ransonware-practical and legal considerations for confronting the new economic engine of the dark web. *Rich. Tech.* **2016**, *23*, 1.
220. Eimer, T.; Luimers, J. Onion governance: Securing drug transactions in dark net market platforms. Paper presented at the Annual Convention of the Belgian Association for Political Science (VPW) and the Dutch Political Science Association (NKWP), Antwerp, Belgium, 13–14 June 2019.
221. Adorjan, M. *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs. By James Martin*; The British Journal of Criminology, Volume 55, Issue 4; Springer: Berlin, Germany, 2015; pp. 835–836.
222. Sutanrikulu, A.; Czajkowska, S.; Grossklags, J. Analysis of Darknet Market Activity as a Country-Specific, Socio-Economic and Technological Phenomenon. In Proceedings of the 2020 APWG Symposium on Electronic Crime Research (eCrime), Boston, MA, USA, 16–19 November 2020; pp. 1–10.
223. Howarth, J.; Smith-Jackson, T.; Hartson, R. Supporting novice usability practitioners with usability engineering tools. *Int. J. Hum. Comput. Stud.* **2009**, *67*, 533–549. [CrossRef]
224. Clark, J.; Van Oorschot, P.C.; Adams, C. Usability of anonymous web browsing: An examination of tor interfaces and deployability. In Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 18–20 July 2007; pp. 41–51.
225. Das, S.; Dingman, A.; Camp, L.J. Why Johnny doesn't use two factor a two-phase usability study of the FIDO U2F security key. In Proceedings of the International Conference on Financial Cryptography and Data Security, Nieuwpoort, Curaçao, 26 February–2 March 2018; pp. 160–179.
226. Miesenberger, K.; Edler, C.; Heumader, P.; Petz, A. Tools and applications for cognitive accessibility. In *Web Accessibility*; Springer: Berlin, Germany, 2019; pp. 523–546.
227. Leduc-Mills, B.; Dec, J.; Schimmel, J. Evaluating accessibility in fabrication tools for children. In Proceedings of the 12th International Conference on Interaction Design and Children, New York, NY, USA, 24–27 July 2013; pp. 617–620.

228. Gallagher, K.; Patil, S.; Memon, N. New me: Understanding expert and non-expert perceptions and usage of the Tor anonymity network. In Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), Santa Clara, CA, USA, 12–14 July 2017; pp. 385–398.
229. Rates, R.; Default, L.G. A false Sense of Security. *Risk* **2003**, 63–67. Available online: https://www.chicagofed.org/-/media/publications/risk-management-papers/sr-2005-1-pdf.pdf (accessed on 30 March 2022).
230. Steinebach, M.; Zenglein, S.; Brandl, K. Phishing detection on tor hidden services. *Forensic Sci. Int. Digit. Investig.* **2021**, *36*, 301117. [CrossRef]
231. Abawajy, J. User preference of cyber security awareness delivery methods. *Behav. Inf. Technol.* **2014**, *33*, 237–248. [CrossRef]
232. Cuchta, T.; Blackwood, B.; Devine, T.R.; Niichel, R.J.; Daniels, K.M.; Lutjens, C.H.; Maibach, S.; Stephenson, R.J. Human Risk Factors in Cybersecurity. In Proceedings of the 20th Annual SIG Conference on Information Technology Education, Acoma, WA, USA, 3–5 October 2019; pp. 87–92.
233. Kethineni, S.; Cao, Y. The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *Int. Crim. Justice Rev.* **2020**, *30*, 325–344. [CrossRef]
234. Ghappour, A. Searching places unknown: Law enforcement jurisdiction on the dark web. *Stan. L. Rev.* **2017**, *69*, 1075. [CrossRef]
235. Rafiuddin, M.F.B.; Minhas, H.; Dhubb, P.S. A dark web story in-depth research and study conducted on the dark web based on forensic computing and security in Malaysia. In Proceedings of the 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 21–22 September 2017; pp. 3049–3055. [CrossRef]