Hindawi
Journal of Computer Networks and Communications
Volume 2021, Article ID 1302999, 21 pages
https://doi.org/10.1155/2021/1302999

Review Article

Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence

Randa Basheer [1] **and Bassel Alkhatib** [1,2]

[1]*Faculty of Information Technology and Communications, Syrian Virtual University, Damascus, Syria*
[2]*Faculty of Informatics Engineering, Al-Sham Private University, Damascus, Syria*

Correspondence should be addressed to Randa Basheer; randa_151689@svuonline.org

Received 3 September 2021; Revised 30 October 2021; Accepted 2 December 2021; Published 20 December 2021

Academic Editor: Zhiyong Xu

From proactive detection of cyberattacks to the identification of key actors, analyzing contents of the Dark Web plays a significant role in deterring cybercrimes and understanding criminal minds. Researching in the Dark Web proved to be an essential step in fighting cybercrime, whether with a standalone investigation of the Dark Web solely or an integrated one that includes contents from the Surface Web and the Deep Web. In this review, we probe recent studies in the field of analyzing Dark Web content for Cyber Threat Intelligence (CTI), introducing a comprehensive analysis of their techniques, methods, tools, approaches, and results, and discussing their possible limitations. In this review, we demonstrate the significance of studying the contents of different platforms on the Dark Web, leading new researchers through state-of-the-art methodologies. Furthermore, we discuss the technical challenges, ethical considerations, and future directions in the domain.

1. Introduction

In the age of technology, and with the rapid development of hacking techniques and tools, it has become an urgent need for various organizations to take appropriate countermeasures against cyberattacks and cybercriminals. Moreover, proactive detection of cybersecurity threats is one of the fundamental and challenging actions needed to anticipate and detect an attack before it occurs. Cybersecurity attacks can come in different patterns and levels, differing in their complexity, breadth, and objectives. This vast diversity necessitates institutions and countries in general to make cybersecurity one of their essential systems.

Because of the rapid technical development, a large part of hacking activities transformed from just individual acts of theft and vandalism to well-organized and financially supported actors aiming for profits on a large scale. The objectives of organized crime in this domain range from financial gain to achieving political goals [1].

This transformation urges organizations to consider contemporary and sophisticated techniques to keep pace with the development of cyberattacks. Therefore, a new in-demand generation of cybersecurity tools is arising and attracting increasing interest from researchers and security practitioners, which is Cyber Threat Intelligence (CTI). CTI is an information system that provides evidence-based knowledge about cyber threats. Considering the gained knowledge, organizations can make cybersecurity decisions, including detecting, preventing, and recovering from cyberattacks [1].

Recently, and in light of the COVID-19 pandemic outbreak, the number of data security attacks has increased dramatically, as the pandemic has forced a state of work-at-home applied by organizations worldwide without taking adequate and effective measures against these attacks [2]. In another COVID-19-related aspect, hacking communities witness an increase in posts discussing exploiting the pandemic as a new opportunity for attacks, most notably of which attacks targeting remote work tools and fraudulence that target people looking for jobs or information about COVID-19 [3].

Social networks on Deep and Dark Webs are considered essential places where hackers can gain technical

information and develop their skills. On such networks, they share information, communicate with each other, and sell hacking-related materials such as breached data, stolen card numbers, and system vulnerabilities [4]. Criminal networks rely on social ties in their formation and growth. On the Internet, social networks, forums specifically, provide similar intellectual affinity of criminals, such as hackers, to exchange information and experiences or plan for crimes and attacks [5].

In these platforms, members can follow posts from other members that they consider trustworthy or experts. Moreover, forum members have different specializations and rankings within the same community according to their activities and services. Therefore, forums provide the proper environment for the growth of cybercriminals networks and increase opportunities for planning and conducting cybercrime worldwide [5]. Consequently, these places provide vital resources for researchers and cybersecurity experts to detect cyberattacks early and provide organizations with warnings of potential threats [4]. Moreover, studying these hackers' communities on the Dark Web allows for the continuous development of new areas in security informatics technologies [6].

In this review, we highlight the importance of analyzing content on Dark Web platforms to detect and predict cybercrimes, leading new researchers through previous works. We introduce a comparative study of recent researches, their research goals, approaches, used methods and tools, applied case studies, and results, and discuss their possible limitations. Furthermore, this review highlights notable challenges in analyzing Dark Web content, emerging fields, and future directions. We excluded studies in crawling or collecting data from Dark Web or present only statistical analysis approaches. We focus on studies that analyze the content of Dark Web platforms (such as websites, forums, social networks, marketplaces) to gain valuable information for Cyber Threat Intelligence (CTI) (Abbreviations: social network analysis (SNA), content analysis (CA), artificial intelligence (AI), machine learning (ML), data mining (DM), natural language processing (NLP), topic modeling (TM)).

2. Related Work

It is worth mentioning and directing the interested reader to other surveys in the domain of CTI in general. In these surveys, researchers can find the description of different threat intelligence types and information-sharing strategies with a comparative study of the most popular open-source threat intelligence tools and declaration of technical and nontechnical challenges [7, 8]. Moreover, an analysis of the current role of the Dark Web as an environment that facilitates cybercrime and illicit gain can help understand the particularity of the Dark Web [9], in addition to the importance of knowledge and employment of DM and ML methods to predict and discover patterns of cyberattacks [10]. An extensive description of possible cybersecurity data sources and applications can support launching cybersecurity studies [11]. Researchers can leverage a detailed explanation of CTI types and their phased cycles with the application of AI and ML methods for prompt, actionable operations [12]. An overview of existing CTI platforms and their approaches and information provision abilities can help researchers find current gaps to start with and provide improvement to the CTI industry [13].

3. The Particularity of the Dark Web

To begin with, we present a simple explanation of the Internet layers down to the Dark Web, while explaining these layers in detail is out of the scope of this review.

First, the Surface Web (Open Web or Clear Web in other synonyms) represents all websites that are publicly and easily accessible because search engines can index them. Alternatively, numerous websites are inaccessible because search engines cannot index them, forming the Deep Web (or the Invisible Web). In the latter, one needs to type the URL of the website directly in the address bar of the web browser, or the website itself is visible but its content needs a password to access it [14].

Researchers should differentiate Deep Web from Dark Web. The Deep Web is part of the web that search engines cannot access for different reasons related to the operational functions of the websites. Researchers estimate this part at more than 90% of the entire web, whereas the Dark Web is part of the Deep Web that uses special encryption software to hide users' identities and IP addresses [15].

Thus, the most difficult-to-access part of the Deep Web is the Dark Web or the Darknet in another synonym. This anonymization leads to the predominance of malicious and criminal activities in that hidden and encrypted environment [15]. Various crimes and heinous actions are prevalent in this part of the web, including novice and professional hackers either for fun deeds or for making gains through extortion, sabotaging networks, or stealing organizations' data, in addition to many crimes such as children pornography and pedophile networks, drugs and arms trade, human trafficking, terrorism and recruitment of extremists, planning terrorist attacks, murderers for hire, hacked digital media trade, counterfeit documents, fraud, and many others [15, 16].

The Dark Web provides the ability to hide the user's identity, network traffic, and data exchanged through it. Users outside the Dark Web cannot access it using standard web browsers but through special software, such as The Onion Router (TOR), Invisible Internet Project (I2P), and Freenet [15, 17]. Researchers consider dark networks the primary host for various criminal activities. For example, marketplaces on the Dark Web are evidence of Crime-as-a-Service (CaaS), as they provide most of the items commonly found in conventional black markets [18]. Trades on Dark Web marketplaces are anonymized as well, where members complete their transactions using cryptocurrencies, such as Bitcoin and Monero [16]. In this regard, some cybercriminals act as cryptocurrency providers to make it easier for others to perform criminal activities [19].

In terms of cybersecurity threats, hacking communities are active on Dark Web platforms, where hackers exchange

experiences and share information, in addition to circulating hacking tools, malware, ransomware, breached data, and planning large-scale cyberattacks resembling a pattern of an organized crime [16].

Alternatively, Dark Web marketplaces are fraught with hacking products and tools for organizing attacks. Additionally, vendors offer breached personal data, such as credit cards, bank accounts, PINs, credentials, and other Personal Identifiable Information (PII). These marketplaces also provide botnets for renting to perform Distributed Denial of Service (DDoS) and fraud and spam services such as e-mail lists for sending phishing e-mails [14].

Dark Web marketplaces include sellers and buyers with different levels of technical expertise. For example, a small class of highly experienced professional sellers creates and sells sophisticated hacking tools and malware, whereas other less-experienced members buy from or collaborate with them to organize massive attacks or breached data exploitation in a Crime-as-a-Service (CaaS) paradigm. This example of crime indicates that technical professionalism is no longer an essential component to conduct cybercrime [14]. In this context, some professional vendors offer security services to others to provide an extra level of protection and privacy against law enforcement agencies' operations. Thus, if a cyberattack is detected, the identity of the perpetrator remains unknown [14].

In this regard, studies have shown that many successful cyberattacks relied on the cohesion of the mutual relationships between the hackers, which they established in the long term of cooperation, especially with the different levels of skills they possess. These levels entail them cooperating to implement the attacks and achieve their pursued gains. Therefore, these networks and marketplaces form what look like peership or colleagueship networks [19].

Moreover, many cybercrime marketplaces operate alongside hacking forums. Sellers advertise their products on these forums along with a description of the product features, price details, payment methods, terms of services, and contact information of the seller. For the latter, sellers and buyers tend to use other encrypted communication media such as private messaging apps or direct messaging features included in the forum [14]. Dark Web marketplaces play a significant role in providing hacking-related items. From the existence of markets for hackers, one can infer that the focus of such business on the Dark Web is financial gains, which are sometimes monopolized by the professional minority that dominates the market [20].

Some forums maintain a level of professionalism by establishing a reputation system to prevent intruders or, in the case of researchers, from gathering information. The reputation system is based on giving professional and active users in the community more privileges as their professionalism and trustworthiness levels increase, such as getting more reputation points and permission to access other sections in the forum [3].

TOR also allows hosting websites, thus masking the location of the hosting servers, or TOR Hidden Services, and they can only be accessed through TOR [14]. Recently, Darknets have become more complex and difficult to penetrate. TOR has added a layer of privacy in 2017 that increases the complexity of identifying both website hosts and visitors. Thus, platforms on the Dark Web will be less discoverable. Moreover, website administrators become more inclined toward making sites and forums accessible by invitation only [16].

Conventional cybersecurity solutions have focused on protecting endpoint devices of all kinds; however, while they can be effective for some time, they are not a long-term remedy [16].

On the bright side, methods and techniques of artificial intelligence, machine learning, data mining, and analytics are vital tools in fighting cybercrime. Such tools assist law enforcement agencies to target and disrupt websites on Dark Web. Additionally, they provide them with the legal evidence they need to sanction perpetrators [16].

It is worth noting that not all activities on the Dark Web are illegal; many entities use encryption software for legitimate purposes, such as journalists, political activists, whistleblowers, and law enforcement agencies and researchers for research purposes [15, 16].

4. Dark Web and CTI

As discussed previously, Dark Web represents a critical source of information for CTI. In this section, we first start with a brief description of CTI with different aspects. Then, we introduce a review of recent researches, comparing their objectives, approaches, used methods and tools, results, and possible limitations.

4.1. Cyber Threat Intelligence (CTI). Cyber Threat Intelligence (CTI) is an information system that supports public and private organizations to detect, identify, monitor, and respond to cyber threats. This acquired information helps to understand the tactic, techniques, and procedures (TTPs) of threats and threat actors. Moreover, it provides organizations timely security alerts, recommended settings, and other information according to the type and purpose of the CTI system [21].

CTI provides information related to customary five questions: Who, What, Where, How, and When. CTI can leverage data from multiple sources. Sources can be internal (such as network events log files, firewall logs, alerts, responses to previous incidents, the malware used for attacks, and network flows), or external (such as reports from other institutions or governments, and experts' blogs) [21].

According to Sari, an effective and efficient CTI should have five major characteristics: timely, relevant, accurate, specific, and actionable [21].

CTI includes several subcategories according to its purpose and sources. For example, there are Open-Source Intelligence (OSINT), Social Media Intelligence (SOCMINT), Measurement and Signature Intelligence (MASINT), Human Intelligence (HUMINT), and Technical Intelligence (TECHINT). Sari [21] addressed in detail each type of CTI for further reading. Alsmadi [22] added other examples like Communication Intelligence (COMINT),

Deep or Dark Web Intelligence, Signal Intelligence (SIGINT), and Geospatial Intelligence (GEOINT).

Alsmadi [22] defined three levels of Cyber Intelligence:

(1) Strategic Cyber Intelligence, which is responsible for identifying threats in terms of sources, objectives, and possible consequences

(2) Operational Cyber Intelligence, which provides information about attackers' capabilities and resources, and predicts targets and methods employed by actors to achieve their goals

(3) Tactical or Technical Cyber Intelligence, which provides information about real-time methods and tools used by attackers, and addresses the countermeasures and defending strategies to be followed by organizations

Several informational aspects from the Dark Web can help form a defense and remedy against cyberattacks. These aspects can include analyzing a recent attack on a specific organization, tracking changes on hacker marketplaces, monitoring hackers' behavior on hacking communities, and evaluating the developments in hackers' skills and capabilities [23]. Indeed, Shakarian [23] classified CTI into four tires (illustrated in Figure 1): (1) situational awareness, (2) imminent threats, (3) understand capabilities, and (4) understand communities, in which he gives the upper tiers (third and fourth) great importance for long-term considerations.

CTI is primarily a data-driven process; therefore, it needs several stages to collect, process, and analyze data according to the security needs of the organizations (public, private, or cybersecurity specialized). To understand the intelligence an organization requires, it should acquire several components, including inspecting the existing security domain, determining the current cyber threats, monitoring its cyber assets, and modeling potential directions of future threats [13].

Generally, CTI has four stages illustrated in Figure 2 [13]:

(1) Intelligence planning/strategy

(2) Data collection and aggregation

(3) Threat analytics

(4) Intelligence usage and dissemination

4.2. Dark Web Analysis in the Field of CTI. We organize reviewed researches listed below based on the leading issues they cover, although some studies fall under multiple subjects.

4.2.1. Detecting and Predicting Cyber Threats. Sapienza [24] presented an approach that integrates information from social networks on Surface, Deep, and Dark Webs. The system matches discovered terms from posts of cybersecurity experts on social media (Twitter) and hackers' discussions on Dark Web forums to generate warnings about anticipated or current cyber threats. The system identifies important terms using text mining techniques and computes their occurrences in Dark Web hacking forums. Additionally, the system connects the resulting terms with a group of words that have contextual semantic relationships with these terms for further interpretation and enriching the perception of the warning and eventually tracking and observing the evolution of activities related to the discovered terms on the Dark Web.

Working on already discovered vulnerabilities, Almukaynizi et al. [25] introduced an approach that maps multiple resources, such as white-hat community, vulnerability research community, and websites on the Dark Web and Deep Web, to predict if hackers will exploit a vulnerability. The approach highlights how the likelihood of exploitation increases when the associated vulnerability has frequent mentions in the resources at study.

In another work, Almukaynizi et al. [26] introduced the DARKMENTION system that employs association rules to find correlations between threats mentioned on Dark and Deep Webs and real-world cyber incidents. By using the discovered correlations, the system generates warnings to cybersecurity organizations promptly. The approach depends on Causal Reasoning concepts and Logic Programming (specifically Point Frequent Function (PFR)) to learn the rules.

Williams et al. [27] introduced an incremental crawling approach that crawls, classifies, and visualizes cyber threats. The classification phase categorizes up-to-date hacking exploits and attachments, detects trending and emerging threats, and analyzes hackers' activities by year and exploit type.

Using ontologies, Narayanan et al. [28] proposed a framework that provides cybersecurity experts with semantically enriched knowledge representation and reasoning with the aim of early detection of cyberattacks. The approach relies on the fact of information incompleteness, considering that security blogs and discussions on the Dark Web are often written for a specific audience (such as alike minds or fellows of expertise). The system analyzes data about previous attacks patterns, tools used for these attacks, and other indicators as the reasoning part of the system to detect known and unknown attacks. Furthermore, the system employs association rules and clustering techniques to find complex patterns of events in the data stream.

Tavabi et al. [29] proposed DarkEmbed, a framework with a neural language modeling approach to predict the exploitation of vulnerabilities. The framework represents discussions from the Dark Web and Deep Web forums in low-dimensional vector space by employing language embeddings, which find the contextual, syntactic, and semantic relationships between words, and then using the distributed representations as classification features.

Arnold et al. [30] developed a CTI tool to identify cyber threats by analyzing social network data on the Dark Web to detect valuable information relevant to the diffusion of malicious tools and services, their key actors and participants, and breached data. Based on text feature analysis, the approach integrates text analytics from both forums and marketplaces on the Dark Web to gain information from actors' discussions and interactions and information about the actual traded products (breached data). Key actors post

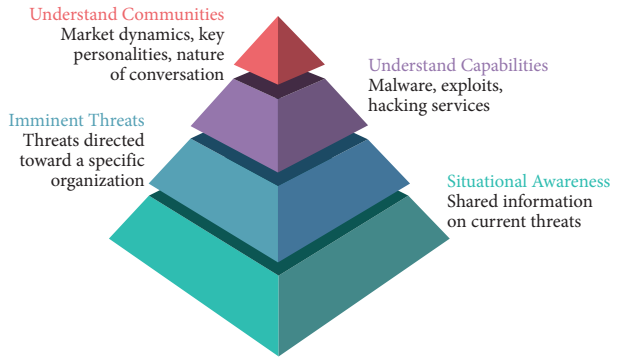

Figure 1: Tiers of Cyber Threat Intelligence (CTI) as classified by Paulo Shakarian [23].

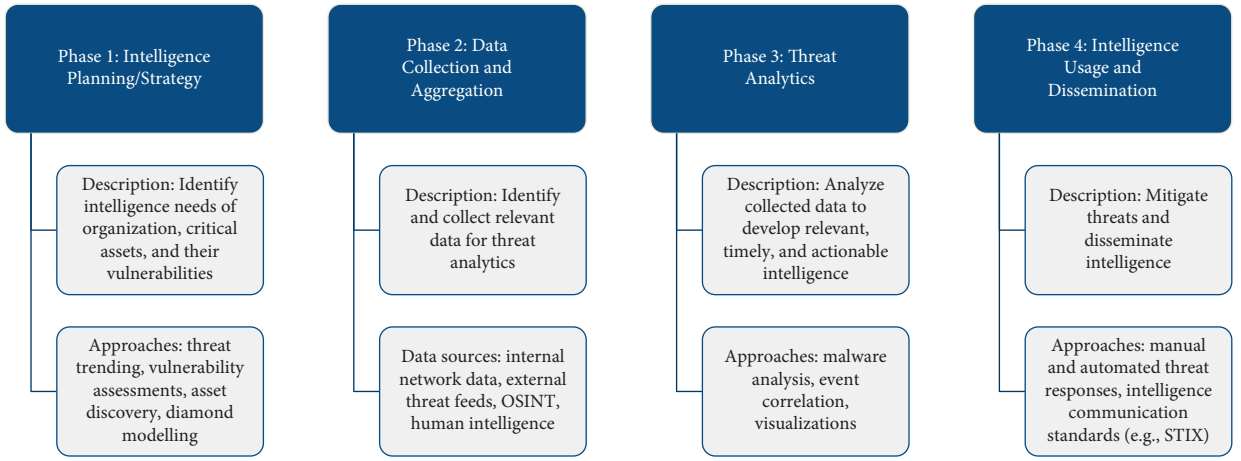

Figure 2: General Cyber Threat Intelligence (CTI) Lifecycle as demonstrated by Samtani et al. [13].

diverse contents that contain contextual and temporal information related to their offers on the markets. Thus, the authors confirmed that considering forum data is substantial, as they are rich in text.

In classifying the source code, Ampel et al. [31] presented an approach to classify exploits source code based on deep transfer learning methodology. Their Deep Transfer Learning for Exploit Labeling (DTL-EL) tool takes the labels identified by professionals from public exploit repositories and performs a generalization on exploits extracted from hacker forums with enriching metadata. Furthermore, the system classifies the gained information in predefined categories to conduct proactive measures by cybersecurity organizations. The approach takes advantage of metadata and categories found in specific Dark Web marketplaces, forums, and public repositories.

The INTIME tool in Koloveas et al.'s work [32] provides a framework to identify and analyze cyber threats in specific cybersecurity topics (Internet of Things (IoT)) to share knowledge among cybersecurity organizations. Their approach integrates information extracted from Surface, Deep, and Dark Web resources, including websites, forums, marketplaces, social networks, and databases published by security agencies to enrich the gained data. The tool performs several tasks such as data collection, usefulness ranking, identifying cyber threats, linking different acquired information, and sharing the resulting cyber threat intelligence. These tasks utilize specific crawlers, social network monitors, NLP techniques, ML methods, named-entity recognition, and semantic correlations and similarity.

4.2.2. Analyzing Hacker Behavior and Detecting Key Actors. Samtani et al. [33] introduced a CTI framework that focuses on analyzing hackers' assets within forum discussions. The framework utilizes classification and TM on the implementation of disseminated hacking tools. Furthermore, it takes advantage of the available metadata and posts' contents to explore trending tools. The framework applies bipartite SNA to detect key hackers in the communities. The constructed bipartite networks represent the relationship between hackers and threads of specific types of assets and eventually explore key hackers for each extracted topic.

Focusing on mobile malware and key hackers, Grisham et al. [34] introduced a proactive CTI tool to identify mobile malware attachments and their key authors from Dark Web hacker forums in different languages. They employed text classification methods to detect malware using neural network architecture and recurrent neural networks while applying SNA to identify key authors. The tool extracts the textual features from the subforum name, thread title, post content, and the attachment name to classify the malware.

Furthermore, it identifies trending and common malware by distributing the discovered malware over posting date. On the actors' side, they constructed a bipartite author-thread network, projecting it with the authors' network to infer hackers' co-occurrences in a unified network.

Pastrana et al. [35] aim for two objectives in their approach, preventing young people from drifting to become cybercriminals and helping security agencies to take suitable actions in response to cyberattacks. They employ several procedures to understand the behavior pathways of cybercriminals. The system identifies key actors by modeling their shared characteristics based on their forum activities, analyzes their temporal evolution in interests and knowledge, and predicts the probability of some users becoming future key actors. The proposed system utilizes ML, NLP, SNA, and TM. Furthermore, a directed network of replies and citations represented the relationships between actors.

Biswas et al. [36] studied hacker behavior in hacker forums to identify significant predictors that detect key hackers or leaders. They define a hacker community as a community of practice or knowledge community of practice where each member plays a role. Therefore, they employed text mining and sentiment analysis techniques to generate predictors and construct a hacker-role classification model. The study addressed eleven hypotheses and proved the high significance of four: (1) discussion threads to determine hacker expertise, (2) the number of messages posted to classify hackers based on their meritocracy, (3) the number of responses in each thread to classify hackers based on their expertise, and (4) average message size to classify hacker role. Four hypotheses have possible connections with hacker expertise, whereas the other three were insignificant.

Marin et al. [37] introduced an approach to identify key actors and discover unique features of cybercriminals. They employed CA over topics and their authors, SNA to construct interaction graphs and detect communities, and seniority analysis to identify hacker coverage and involvement over time. They utilized the three techniques separately and combined, and validated their results based on reputation systems within hacker forums as a ground-truth dataset. The approach aims at proving how a model learned from one forum can be generalized to identify other forums' key actors.

Marin et al. [38] proposed an approach to predict future posts of hackers by analyzing their adoption behavior. The adoption behavior means how hacking community members adopt the posting topics of influencing hackers and post in the same direction. They employ sequential rule mining to discover members' posting rules by their sequences of posts within defined time windows (day and hour), and then, they use these rules to predict near-future posts.

In a different aspect, Deb et al. [39] suggested using sentiment analysis to support time series modeling in predicting cyber events, tested on ground-truth events from two organizations. Their approach aims at generating predictive signals from hacker forums by analyzing the sentiments dominating forum posts for better understanding hackers' behavior over time.

Zenebe et al. [40] employed descriptive and predicative analysis tools and ML methods to detect cyber threats proactively and identify key actors in hacker forums on the Dark Web. Their approach focused on extracting trending topics among hackers as the most common threats and influential members as key actors, achieved using IBM Watson Analytics and WEKA ML tools.

To analyze hackers' behaviors and strategies and predict the near-future attacks afterward, Marin, Almukaynizi, and Marin et al. [41] proposed a temporal logical framework that learns the rules correlating hacking activities (preconditions) to real-world cyber incidents (postconditions). They used sociopersonal characteristics of the hackers who mention the vulnerabilities (such as hackers' activities, influences, and expertise) and technical attributes of the attacks from the mentioned vulnerabilities (such as recent patches or released exploitation scripts).

Sarkar et al. [42] used information from Dark Web forum posts represented in a graph of replies to predict real-world cyberattacks on specific organizations. They used classification methods over social network features. The suggested approach focused on the dynamics of discussions to extract valuable patterns about how a single piece of information gains popularity among members in a specific timestamp. These patterns can help identify specialized members or experts. Afterward, they apply time series methods to capture the dynamism of other members' interactions on those experts' discussions and link-extracted patterns with real-world security incidents to predict future attacks.

Huang et al. [43] proposed a hybrid method, HackerRank, which combines CA and SNA to detect key hackers. The approach uses CA to extract the topics preferences of forum members, and then, it uses SNA to construct a network representing relationships among members and identifying key hackers. The HackerRank evaluates members' ranking and extracts members with the highest ranks as key hackers. The method constructs the social network graph based on members' interactions (the replies) and evaluates the activeness of a user by the number of posts and replies.

4.2.3. Performance and Optimization. Deliu et al. [44] presented a comparative study of ML methods employed for detecting cyber threats from hacker forums. The study compares performances of convolutional neural network (CNN) and support vector machine (SVM). The comparisons included traditional classifiers with Bag-of-Words features and N-gram features while applying CNN with several feature vectors representing forum posts as sequences of words, using Word Embeddings to preserve the semantics of the words. The approach focuses on filtering out irrelevant posts using optimized classifiers with the highest accuracy for more accurate CTI results.

In another work, Deliu et al. [45] introduced a reduction approach to optimize the TM process of detecting cyber threats from hacker forums. They employed three reduction approaches: (1) classification to filter out irrelevant topics,

(2) reducing the vocabulary size, and (3) reducing the number of topics.

Koloveas et al. [46] used classification and language modeling methods to support the crawling tasks by representing the collected information in a latent low-dimensional feature space, to analyze the content relevant to a specific hacking topic (IoT in the proposed study).

Queiroz et al. [47] proposed an approach to enhance classification models using language models for feature representation. They employed Word Embeddings (WEMB) and Sentence Embedding (SEMB) techniques to find semantic contextual properties of words and sentences, to detect cyber threats and posts related to vulnerabilities in forums and social networks in Surface, Deep, and Dark Webs.

Johnsen and Franke [48] presented two essential suggestions: using OSINT for proactive cyberattacks detection and applying extensive preprocessing on the document corpus iteratively before applying TM. These operations help to extract more coherent and focused topics.

A deep learning approach by Ebrahimi et al. [49] used a semisupervised labeling methodology to reduce manual labeling of training data. The system takes advantage of the lexical and structural characteristics of Dark Web marketplaces to increase classification performance while autodetect cyber threats from hacking listings. The approach uses both Transductive Learning (TSVM) and Deep Bidirectional LSTM networks to identify threats.

4.2.4. Language Variations. The approach of Nunes et al. [50] integrated hackers' discussions on forums and their offerings on marketplaces on the Dark Web for proactive detection of cyberattacks targets, considering different languages. They categorized the targets into three main domains: platforms, vendors, and products. Their tool employs knowledge reasoning techniques that use a hybrid methodology of Defeasible Logic Programming (DeLP) and ML classifiers to reduce classification labels and to gain focused results.

By transferring knowledge from English Dark Web marketplaces to non-English ones, Ebrahimi et al. [51] proposed an approach to detect cyber threats from non-English marketplaces without the need for mono- or bilingual word embeddings or automatic translation. The system utilizes Deep Cross-Lingual Modeling that simultaneously learns common representations from two languages (English and Russian in the study). It generates a shared Bidirectional Long Short-Term Memory (BiLSTM) between English and Russian marketplaces by integrating labeled data from English markets with the limited labeled data from the Russian market. Their goal behind knowledge transfer is to reduce false positives and false negatives.

BlackWidow, a tool proposed by Schäfer et al. [52], discovers the features shared among platforms on both Dark Web and Deep Web to support future cybersecurity problems. The tool analyzes and compares forums in different languages to find cross-relationships, trending subjects, and key authors from multilingual content. Eventually, it constructs a knowledge graph of threads, actors, messages, and topics and the relationships among these four types of nodes. The generated network defines relationships among users by their replies to each other and trending topics by applying time series.

In another work, Ebrahimi et al. [53] suggested that translating non-English texts to English causes loss in the semantics of the language, therefore affecting the classification results. They presented an approach to detect cyber threats from untranslated non-English hacker forums to preserve the original semantics and produce an integrated cross-language knowledge representation about cyber threats from multiple sources in different languages. They proposed the Adversarial CLKT (A-CLKT) approach based on Long-Short-Term Memory (LSTM), Cross-Lingual Knowledge Transfer (CLKT), and Generative Adversarial Networks (GANs) principles.

4.2.5. The Role of Dark Web Marketplaces. Dong et al. [54] introduced a lightweight framework for detecting new cyber threats emerging from Dark Web marketplaces and new releases of already existing threats. The framework applies classification and text mining to the titles and descriptions of offered items to identify new terms that may represent new vulnerabilities or newly released malware. Furthermore, the framework generates warnings from the discovered terms with the associated properties such as vendor name, release date, and keywords.

Marin et al. [55] presented an approach to detect communities of vendors of malware and exploits from Dark Web marketplaces. They addressed the hypothesis that vendors with high similarities will form a community in the real world. The approach employed ML and SNA to prove how multiplexity social ties play an essential role in detecting and validating such communities. For cross-validation of detected communities, they divided a group of marketplaces into two sets and calculated the similarities among vendors according to the number of shared product categories and the corresponding number of products in each category they share. Consequently, they generated two bipartite networks, vendors-products network, and vendors-categories network. Eventually, they projected the generated networks to create a monopartite network of correlated vendors.

Table 1 summarizes the reviewed studies according to their goals, the proposed approaches, utilized methods and tools, case studies, results, and possible limitations (for visibility purposes, we place the limitations below each research row). Table 2 demonstrates topics covered by each research.

5. Challenges and Ethical Concerns

In the linguistics domain, Ferguson [56] addressed some significant challenges when studying the Dark Web content:

(1) Inconsistency of the language used in communications between community members and forum discussions; this inconsistency is intended in Dark Web communities as a type of anonymity procedure.

Table 1: A comparison of reviewed literature according to their goal, approaches, used methods and tools, case studies, results, and possible limitations.

Reference	Research goal	Approach	Used methods and tools	Case study	Results
(Sapienza et al. 2017) [24]	Detecting cyber threats from Surface, Deep, and Dark Webs	(i) Focused Crawling (ii) Text mining (iii) Semantic context	(i) Amazon EC2 (ii) Elastic Search (iii) Twitter API (iv) REST-based API	(i) Twitter posts of 69 cybersecurity experts (ii) 200 Dark Web and Deep Web hacking forums and markets	Generating warnings about specific threats and malware mentioned in Dark Web hacker forums
	(i) Short list of security experts (ii) Lack of dictionaries causing false alarms (iii) Unhandled terms that can be abbreviated or altered intentionally by hackers (iv) The generated warnings are not early enough				
(Almukaynizi et al. 2017) [25]	Predicting vulnerability exploits	(i) Crawling (ii) Binary classification	(i) SVM (ii) RF (iii) NB (iv) LOG-REG	(i) NVD (ii) CVE (iii) ExploitDB (iv) Zero Day Initiative (v) Sark Web and Deep Web marketplaces and forums (in different languages) (vi) Symantec attack signatures (ground truth)	Predicting exploits with a high true-positive rate and low false-positive rate
	(i) The system does not consider the particularity of each organization, its specific needs, and utilized platforms, and thus it depends on fixed thresholds for all exploitation types (ii) limited ground truth				
(Almukaynizi, et al., 2018) [26]	Predicting Cyber Attacks	(i) Focused Crawling (ii) Association Rules (iii) Causal Reasoning concept (iv) Logic Programming	(i) Annotated Probabilistic Temporal Logic (APT-logic) (ii) Point Frequent Function (pfr)	(i) CYR3CON Dark Web marketplaces and forums (ii) NVD (CVE, CPE)	Generating timely warnings about cyber threats
	(i) Low average of warning trigger time before the attack (3 days) (ii) Lack of performance evaluation according to the consumed time (using n ∗ n matrix of -1 ∗ Lead-time - without a clear evaluation for larger numbers of warnings)				
(Williams et al. 2018) [27]	Proactive detection of cyber threats from forum attachments	(i) Crawling (ii) Classification (iii) Visualization	(i) Python libraries (requests_html, BeautifulSoup, Keras) (ii) RNN (iii) Standard RNN (iv) Gated recurrent unit (GRU) RNN (v) LSTM RNN (vi) Tableau	Ten hacking forums on the Dark Web in different languages	(i) Detecting trending and emerging hacking exploits (ii) Detecting top active authors and top active forums (iii) Classifying exploits and attachments (iv) Analyzing author activities by year and exploit
	Excluding attachments uploaded on third party platforms, thus the system cannot be generalized on forums that prevent direct attachments within posts or can miss some valuable insight within the same forum				

Table 1: Continued.

Reference	Research goal	Approach	Used methods and tools	Case study	Results
(Narayanan et al. 2018) [28]	Detecting cyber event patterns and predicting future cyberattacks	(i) Ontology enrichment (ii) Knowledge graph representation and reasoning (iii) Association Rules (iv) Clustering	(i) Unified cybersecurity ontology (UCO) (ii) Named-entity recognizer (NER) (iii) RDF, OWL (iv) Semantic web rule language (SWRL) (v) Hidden Markov model (HMM) (vi) JENA reasoner	(i) Structured information (threat intelligence sources like US-CERT and Talos) (ii) Plain text (blogs, Twitter, Reddit, Dark Web forums) (iii) CVE	(i) Constructing an enriched cybersecurity knowledge graph to detect cybersecurity events patterns and predict future cyberattacks (ii) Reducing the cognitive load on the analyst (iii) Proving a solution for information incompleteness
	(i) Fewer indicators cause less confidence for attacks that do not follow the seven steps of the intrusion kill chain (ii) Multiple ontologies can produce more accurate results; the approach does not consider the need for a special ontology of hackers' special technical terms and abbreviations, or the use of foreign languages				
(Tavabi et al. 2018) [29]	Predicting vulnerability exploits	(i) Focused Crawling (ii) Language Embeddings (iii) Classification	(i) Paragraph Vector (ii) SVM (iii) Radial basis function (RBF) (iv) RF	(i) Deep Web and Dark Web sites in 17 different languages (ii) ExploitDB, NVD (CVE), attack signatures from Symantec antivirus and Intrusion Detection Systems, and Exploits database by Metasploit (ground truth)	(i) Achieving low-dimensional space (ii) Better classification performance with embeddings
	(i) Lack of ground truth (ii) Sparse data with the higher dimensionalities of feature space (iii) Needs enriched representations for features in other languages				
(Arnold et al. 2019) [30]	Detecting and predicting vulnerability exploits (breached data)	(i) Crawling (ii) Classification (i) SNA (iii) Graph building, annotation, and visualization	(i) *Python* libraries (ii) Gephi	5 largest markets and 3 major forums on the Dark Web	Better performance by integrating SNA on text from both forums and markets on the Dark Web to detect and predict exploits
	(i) Unhandled inconsistency of listing names led to few classification results; thus, a manual search using SQL queries was needed (ii) Lack of real-world evaluation				
(Ampel et al. 2020) [31]	Classifying hacker exploit source codes	(i) Crawling (ii) Deep transfer learning (DTL) techniques	(i) CBiLSTM models (ii) Transferred Embedding (iii) Convolutional and BiLSTM layers	(i) Hacker forums: 8 English, 3 Russian (ii) 1 marketplace: English (iii) Public repositories: English: Seebug, ExploitDB, Packet Storm, Metasploit, Vulnerlab, Zeroscience	Better labeling of exploit source code with DTL than non-DTL techniques
	(i) Low rates of accuracy in some experiments, can be enhanced by considering more features from metadata				

Table 1: Continued.

Reference	Research goal	Approach	Used methods and tools	Case study	Results
(Koloveas et al. 2021) [32]	Identifying, analyzing, and sharing information about cyber threats	(i) Focused and topical crawling (ii) Social media Monitors (iii) Classification (iv) NoSQL storage (v) Predictive and suggested search (vi) Visualization	(i) NYU's ACHE crawler (ii) SMILE classifier (iii) MongoDB (iv) SVM, RF, NB, K-NN, DT, LOG-REG, CNN (v) Gensim (Word2Vec) (vi) spaCy (vii) MySQL (viii) MISP's UI (ix) PyMISP library (x) Stack Exchange data dump	(i) Crawled platforms on Surface, Deep, and Dark Web (ii) Integrated datasets: KB-Cert Notes by Carnegie Mellon University, ExploitDB, VulDB, 0 day Today, NVD (CPE, CVE ID), JVN (JVN iPedia, CPE, CVE ID)	A hybrid CTI tool to detect, identify, analyze, search, and share information about cyber threats
	(i) Downloading of the entire webpages can cause a heavy load on storage (ii) Some domain-specific terms used in the nontechnical text are missed from the named-entity recognizer (iii) Low-quality seed pages for the topical crawler classification model caused false negatives and missing potential important relevant out-links (v) Low rates of precision and recall in the social media monitoring system				
(Samtani et al. 2017) [33]	Classifying hacker assets and detecting key hackers	(i) Crawling (ii) Classification (iii) Web, data, and text mining (iv) Source code topic extraction (v) SNA	(i) SVM (ii) LDA (iii) Bipartite networks (iv) RapidMiner LIBSVM package	(i) 7 Dark Web hacking forums (English and Russian)	(i) Identifying hacker disseminated tools in Dark Web hacking forums, their types, and their functionality features (ii) Detecting key hackers
	(i) Downloading full webpages can cause a heavy load on storage (ii) Some preprocessing procedures may cause losing semantics or names of specific threats (iii) Limited data needed to understand relationships among hackers leading to a small density and low average path lengths of the constructed graph and thus can cause missing some key hackers				
(Grisham et al. 2017) [34]	Proactive detection of mobile malware attachments and key hackers	(i) Crawling (ii) Text classification (iii) Neural network (iv) SNA	(i) Keras (ii) LSTM RNN (iii) Adam optimizer	4 Dark Web hacker forums in different languages	Identifying mobile malware attachments and key authors from Dark Web hackers' forums
	(i) Concentrating on key hackers that only post attachments can miss important key hackers that interact with the other hackers' attachments or perform the attached malware (ii) Lower rates of precision and recall for the model on mobile malware attachments than on nonmobile malware ones				
(Pastrana et al. 2018) [35]	Detecting cyber threats, key actors, predicting potential future key actors, analyzing actors' evolution of interests and knowledge	(i) SNA (ii) Clustering (iii) Topic Analysis (iv) Prediction (v) Classification	(i) SNA network metrics (ii) NLP (iii) Linear SVM (iv) K-means (v) LOG-REG (vi) LDA	Hackforums from CrimeBB dataset	(i) Detecting key actors and their relationships (ii) Identifying actors' behavior pathways and interest transition (iii) Detecting potential cybercrime actors
	(i) Manual search of key actors, thus the approach may not be generalized or scalable (ii) Manually analyzing the activity of neighboring key actors (iii) Low key actors prediction rate (iv) Low-resource language corpora may not be adequate for applying NLP tools (v) Lack of validation of the prediction results				

Table 1: Continued.

Reference	Research goal	Approach	Used methods and tools	Case study	Results
(Biswas, mukhopadhyay, and gupta, 2018) [36]	Analyzing hacker behavior, clarifying hacker roles	(i) Text Mining (ii) Sentiment Analysis (iii) Classification	(i) TF-IDF with overlap score Measure (ii) LOG-REG (iii) SentiStrength	HackHound forum, retrieved from the University of Arizona Hacker database	(i) Discovering predictors in hacker behavior to detect leaders in the community (ii) Building a hacker dialect lexicon (iii) Generating a role-based hacker classification model (iv) Better accuracy
	(i) The results may be affected by the language styles used in the specific platform at study; thus, the approach needs the proved hypotheses to be validated on other platforms (ii) Low rate of precision and recall for some predicted hack roles				
(Marin, shakarian, and shakarian, 2018) [37]	Detecting key hacker in Dark Web hacking forums	(i) CA (ii) SNA (iii) Seniority Analysis (iv) Classification (v) Prediction	(i) Genetic Algorithms (ii) LR (iii) RF (iv) SVM	3 hacker forums on Dark Web (English)	(i) Identifying key hackers (ii) Generalizing the model on other forums that do not have reputation systems (iii) Achieving better performance with a hybrid approach and combined features
	(i) The compared forums have wide distinctions of reputation values (134, 102, and 37); thus, this may affect the results of training and testing processes conducted alternately between them (as shown in the study results when using Forum 3 in the testing). (ii) Low rates of identified key hackers (0.52 as the highest value) (iii) Lack of validation on the same forum: the approach was trained and tested on different platforms but not on the same platform				
(Marin et al. 2018) [38]	Predicting hackers' future post topics	Sequential rule mining	TRuleGrowth algorithm	A popular hacking forum on Dark Web	Detecting members' adoption behavior of topics posted after getting influenced by their peers
	The approach needs a justification for using hours' granularity for sequential rules generating and prediction, while the hours' granularity has double numbers of rules of those of the days' granularity, with low precision rates. This insight can be misleading as the rules generated for the hours within the same day can be the reason for this increase in rule number (and this cannot be applicable, readable, or adequately visualized)				
(Deb, lerman, and ferrara, 2018) [39]	Predicting future cyber events	(i) Sentiment Analysis (ii) Time-series prediction	(i) VADER (ii) LIWC15 (iii) SentiStrength (iv) ARIMA (v) Apache Lucene's elastic search engine	113 hacking forums in English on the Surface and Dark webs, provided by CYR3CON	(i) Predicting cyberattacks weeks before the event (ii) Exploring the relationship between community behavior and cyber activity (iii) Determining the forums with more predictive power than other forums
	(i) Low performance of the sentiment signal system for low frequencies (small numbers of events) (ii) The performances resulted differs according to the attack type; thus, the system's performance needs to be validated on other types of attacks (iii) Low precision and recall rates for some dominated months				

Table 1: Continued.

Reference	Research goal	Approach	Used methods and tools	Case study	Results
(Zenebe et al. 2019) [40]	Proactive detection of cyber threats and identifying key hackers	(i) Classification (ii) Prediction (iii) Visualization	(i) IBM Watson Analytics (ii) WEKA (iii) RF (iv) RT (v) NB	University of Arizona's Artificial Intelligence Lab dataset	Detecting trending topics and key actors
	(i) Low-quality comparison of top authors in all three forums at study combined, not in the same forum, which can miss the influencing power of each forum on its own (ii) Overfitting of exploits with most of the samples in the dataset (iii) Low accuracy for exploits with a little number of entities (iv) Does not classify irrelevant posts (nonthreat), which can affect the accuracy of classification results				
(Marin, almukaynizi, and shakarian, 2019) [41]	Predicting cyber threats, learning hackers' strategies	(i) Association rules (ii) Causal reasoning (iii) Logic programming	(i) Annotated probabilistic temporal logic (APT-logic) (ii) Existential Frequent Function (EFR)	(i) 53 Dark Web hacking forums retrieved from CYR3CON, in different languages (ii) NVD (CVE, CPE) (iii) ExploitDB (iv) 230 records from an enterprise's logs (ground truth)	(i) Detecting hackers' attack strategies (ii) Predicting near-future cyberattacks
	(i) Ground-truth incident data gained from one enterprise, thus providing a little number of incidents for proper testing. Therefore, it needs validation on other enterprises as each one may face different types of attacks (ii) Most CVE entries are not frequently mentioned in hacking posts (iii) For the mapping with CPE solution followed for the previous issue, most CPEs have a little number of CVE associated with them, which cannot make a complete ground-truth testing data (iv) Low performance of the designed algorithm for higher numbers of predicates (v) Low interval of warning of predicted attack (3 days)				
(Sarkar et al. 2019) [42]	Predicting real-world cyberattacks through analyzing forums discussion posts and replies	(i) Classification (ii) prediction	(i) TS (ii) LOG-REG	(i) 53 Dark Web forums (ii) CVE (iii) CPE	(i) Predicting cyberattacks by analyzing the activities of expert hackers through reply networks (ii) Better results by analyzing the network paths than with PageRank or the number of posts per user
	(i) The model was trained and tested on data from a single enterprise, which can limit the incidents samples and attack types; thus, the system needs to be validated on other organizations' data				
(Huang et al. 2021) [43]	Detecting key hackers from hacking forums on the Dark Web	(i) Crawling (ii) CA (iii) SNA (iv) TM	(i) LDA (ii) Topic-specific PageRank (iii) SNA graph construction	5 hacking forums	(i) Increasing the coverage rate of the forum higher than applying CA or SNA alone (ii) Identifying key hackers based on their topic preferences and activeness
	(i) Training the LDA model on all of the analyzed forums together can affect the results of influencing key hackers in each forum separately, as interests and influencing power differ from one forum to another (ii) Manual validating the resulting key hackers (top 5) can be inapplicable for a larger number of key hackers (iii) Lack of identifying key hackers in real-time, as they are identified using historical data				

Table 1: Continued.

Reference	Research goal	Approach	Used methods and tools	Case study	Results
(Deliu et al. 2017) [44]	Detecting cyber threats with more accuracy (comparing performances)	(i) Classification (ii) Word embeddings	(i) CNN (ii) SVM (iii) DT (iv) K-NN (v) word2vec (vi) GloVe (vii) scikit-learn python library	Nulled.IO	SVM and CNN lead to better performances
	(i) Analyzing post content without titles; titles comprise useful abstractions of the posts and help for better classification (ii) The resulting comparison of the algorithms' performances was applied to one particular case study, which cannot be generalized, as algorithms perform differently on different datasets. Thus, the system needs validation on other platforms.				
(Deliu et al. 2018) [45]	Detecting cyber threats from hacker forum posts	(i) Classification (ii) TM	(i) SVM (ii) LDA	Nulled.IO	Reducing the time consumed by TM by employing classification first
	(i) Some topics with minority numbers needed manual searching as LDA cannot extract; that is, it cannot be generalized for datasets with partial sparse data				
(Koloveas et al. 2019) [46]	Crawling only the content relevant to a specific hacking topic (IoT)	(i) Crawling (ii) Classification (iii) Semantic language modeling	(i) ACHE Crawler (ii) SVM (iii) MongoDB (iv) Gensim	(i) Websites and forums on the Surface Web (ii) Hacking forums and marketplaces on the Dark Web (iii) Stack exchange data dump	Directing the crawler to fetch only relevant content
	(i) Downloading whole HTML pages can cause heavy load on storage with useless data (ii) The approach seems time-consuming with harvesting a massive volume of websites (about 22K per hour) but with a low percentage (1%) of them considered containing actionable CTI after manual checking by experts, and percentages higher than that (not specified) for Social and Dark Webs. (iii) The crawler depends on the link relevance (words or alt-text of the URL) to decide whether to visit the corresponding website or not, which can miss some valuable sources that are relevant but do not specifically describe the content in the URL				
(Queiroz et al. 2019) [47]	Enhancing classification methods of hacker discussions	(i) Word Embeddings (ii) Sentence Embeddings (iii) Classification	(i) Word2vec (ii) Glove (iii) Sent2vec (iv) InferSent (v) SentEncoder (vi) SVM (vii) CNN (viii) Sci-kit (ix) Keras API for TensorFlow	5 datasets including forums, microblogs, and hacker marketplaces from Surface, Deep, and Dark Webs	Experimental results: SEMB improves SVM, WEMB improves CNN
	(i) High rate of false positive causing low rates of recall; thus, the approach resorted to oversampling with an increased number of positive instances to improve Recall (ii) Classifying the datasets into three classes (Yes, No, and Undecided) does not seem to be justified, as instances classified under the Undecided class were included afterward in the Yes class, which may lead to noise or unclear messages classified as threats				

Table 1: Continued.

Reference	Research goal	Approach	Used methods and tools	Case study	Results
(Johnsen and franke, 2019) [48]	Detecting cyber threats, identifying members' roles and interests	(i) Text preprocessing techniques (ii) TM	(i) Several preprocessing techniques (ii) Python Panda package (i) LDA (iii) Scikit-learn package	Nulled.IO	(i) Understanding what the forum is about (ii) Understanding members' interests and roles (iii) Improving results quality by reducing vocabulary size
	(i) Very low hyperparameters values can lead to a very low convergence rate, which cannot be suitable for real-time CTI (ii) Lack of validation of how interpretable the generated topics are for human analysts (iii) The subject-user-centric construction does not yield significant results (iv) The results focus on the majority of users, which are members with little experience or newbies, while overlooking the highly professional ones				
(Ebrahim et al. 2020) [49]	Semisupervised labeling for cyber threat detection from Dark Web marketplaces	(i) Transductive learning (ii) Semisupervised labeling (iii) Heuristics (lexical and structural marketplace characteristics) (iv) Crawling	(i) LSTM (ii) Transductive SVM (TSVM) (iii) El-Gato (iv) Sindhwani's implementation (for TSVM) (v) Context3.0 library (for LSTM)	7 Dark Web marketplaces	(i) Reducing manual labeling (ii) Reducing false positives and negatives in identifying cyber threats
	(i) For the lexical characteristics, the approach depends on the market naming rules that prevent vendors from purposely including irrelevant words in their listing titles. Therefore, the system does not handle the misleading naming for markets that do not force such a rule. (ii) The excessive tests conducted to achieve the optimal values of the hyperparameters for best performance do not justify how the systems will dynamically keep pace with the evolution of the market, changes in labeling, or the newly added labels (iii) The approach needs to be validated on markets in other languages				
(Nunes, shakarian, and simari, 2018) [50]	Early detection of potentially targeted systems: platforms, vendors, products	(i) Logical argumentation (ii) Classification	(i) DeLP (ii) SVM (iii) RF (iv) NB (v) DT (vi) LOG-REG	(i) 302 forums and marketplaces on the Dark Web in different languages (ii) NVD (iii) CVE (iv) CPE	(i) Improving classification performance by reducing the possible labels with argumentation (ii) Identifying potential at-risk systems (platforms, vendors, and products)
	(i) Low rate of precision and recall for vendor and product components (ii) Lack of sufficient data for training (iii) Misclassification of newly discovered vulnerabilities for new products not known as at-risk systems before				
(Ebrahimi et al. 2018) [51]	Detecting cyber threats from non-English hacker marketplaces on the Dark Web without translating the language	(i) Cross-Lingual Representation Modeling (ii) Deep learning	(i) Deep Cross-Lingual Knowledge Transfer (CLKT) (ii) Bidirectional Long-Short-Term Memory (BiLSTM)	Dark Web marketplaces, 7 English and 1 Russian	(i) Achieving better performance than monolingual or translated models (ii) Reducing false positives and false negatives
	(i) Lack of handling short texts (short products titles) (ii) Lack of validation on other languages and platforms (forums)				

Table 1: Continued.

Reference	Research goal	Approach	Used methods and tools	Case study	Results
(Schäfer et al. 2019) [52]	Detecting trending topics in hacker forums, defining relationships between actors and forums	(i) Crawling (ii) Unsupervised TM (iii) Time series (iv) Knowledge graph constructing	(i) Chrome browser Puppeteer (ii) Scala (iii) Apache Spark analytics framework (iv) Elasticsearch (v) Walktrap community-finding algorithm (vi) LDA	Seven forums, 3 on Dark Web and 4 on Deep Web	A CTI platform that performs real-time tasks: (i) Inferring relationships between authors and forums (ii) Extracting trending topics (iii) Inferring relationships among threads, actors, messages, and topics (iv) Detecting overlapping actors across forums
	(i) Translating languages can cause a loss in the semantics and sentiments of the language (ii) Downloading whole webpages can cause a heavy load on storage with unnecessary data (iii) The analyzed forums are easy to access and the assets are free to acquire without excessive measures of authentication or specific user privileges; thus, the approach does not handle the forums with such difficult measures				
(Ebrahimi et al. 2020) [53]	Increasing the capabilities of multilingual cyber threat detection, cross-language cyber threat knowledge representation	(i) Crawling (ii) language invariant representation (ii) Classification	(i) LSTM (ii) CLKT (iii) Generative adversarial networks (GAN) (iv) BiLSTM (v) NB (vi) SVM (vii) RF (viii) K-NN (ix) Gated Recurrent Unit (GRU) (x) Bidirectional Gated Recurrent Unit (BiGRU) (xi) CNN	4 hacking forums on Dark Web (1 English, 1 Russian, and 2 French)	Improving the performance of classical ML and deep learning methods
	(i) Lack of labeled ground-truth data (ii) Low rates of accuracy and precision for some languages (iii) The small volume of data used for training and testing can affect the performance (iv) It needs validation on other languages and multilingual platforms				
(Dong et al. 2018) [54]	Generating warnings about newly emerged threats and new releases of existing threats from Dark Web marketplaces	(i) Crawling (ii) Classification (iii) Text mining	(i) Scrapy (ii) Elastic search (iii) Multilayer Perceptron (MLP) Classifier	(i) 8 Dark Web marketplaces (ii) AlienVault OTX (for existing threat lists)	Detecting new threats emerging from Dark Web markets, and new releases of exiting threats
	(i) High false positives due to foreign languages words and words specified for use in the Dark Web (original words), misspelling, compound words, and proper names				
(Marin et al. 2018) [55]	Detecting communities of malware and exploits' vendors from hacking-related offerings in Dark Web marketplaces	(i) Clustering (ii) SNA (iii) Community Detection (iv) Community validation	(i) K-means with cosine similarity (ii) Louvain heuristic method (iii) Adjusted rand index (ARI)	20 Dark Web marketplaces (English)	Detecting communities of vendors according to their products and shared categories
	(i) Lack of ground-truth data to validate detected communities with real-world communities (ii) Only cross-validation used to justify the suggested hypothesis				

Convolutional neural networks (*CNN*), defeasible logic programming (*DeLP*), decision trees (*DT*), K-nearest neighbors (*K-NN*), latent Dirichlet allocation (*LDA*), logistic regression (*LOG-REG*), linear regression (*LR*), long-short-term memory (*LSTM*), naive bayes (*NB*), natural language processing (*NLP*), random forest (*RF*), recurrent neural network (*RNN*), random tree (*RT*), social network analysis (*SNA*), support vector machine (*SVM*), time series (*TS*), National Vulnerability Database (*NVD*), Common Vulnerability Enumeration (*CVE*), and Common Platform Enumeration (*CPE*).

Table 2: Major topics covered by the reviewed literature (sorted by year).

Reference	Year	Detecting cyber threats	Predicting cyberattacks	Detecting key actors/community	Hacker behavior	Malicious attachment	Language variations	Machine learning optimization
(Almukaynizi et al. 2017) [25]	2017		✓					
(Deliu et al. 2017) [44]	2017	✓						✓
(Grisham et al. 2017) [34]	2017			✓		✓	✓	
(Samtani et al. 2017) [33]	2017			✓		✓		
(Sapienza et al. 2017) [24]	2017	✓						
(Almukaynizi et al. 2018) [26]	2018	✓						
(Biswas et al. 2018) [36]	2018			✓	✓			
(Deb, lerman, and ferrara, 2018) [39]	2018		✓		✓			
(Deliu et al. 2018) [45]	2018	✓						✓
(Dong et al. 2018) [54]	2018	✓						
(Ebrahimi et al. 2018) [51]	2018	✓					✓	
(Marin et al. 2018) [55]	2018			✓				
(Marin et al. 2018) [38]	2018				✓			
(Marin et al. 2018) [37]	2018			✓				
(Narayanan et al. 2018) [28]	2018		✓		✓			
(Nunes et al. 2018) [50]	2018		✓				✓	
(Pastrana et al. 2018) [35]	2018			✓	✓			
(Tavabi et al. 2018) [29]	2018		✓					
(Williams et al. 2018) [27]	2018	✓			✓			
(Arnold et al. 2019) [30]	2019	✓		✓				
(Johnsen and franke, 2019) [48]	2019		✓					✓
(Koloveas et al. 2019) [46]	2019	✓						✓
(Marin et al. 2019) [41]	2019	✓			✓			
(Queiroz et al. 2019) [47]	2019	✓						
(Sarkar et al. 2019) [42]	2019		✓					
(Schäfer et al. 2019) [52]	2019		✓	✓			✓	
(Zenebe et al. 2019) [40]	2019		✓	✓				
(Ampel et al. 2020) [31]	2020	✓				✓		
(Ebrahimi et al. 2020) [49]	2020	✓						
(Ebrahimi et al. 2020) [53]	2020	✓					✓	
(Huang et al. 2021) [43]	2021			✓	✓			
(Koloveas et al. 2021) [32]	2021	✓						

(2) Weak grammatical, spelling, and idiomatic context (also intended).

(3) Individuals deliberately do not use particular terms or use them only in specific cases and ways.

(4) The cultural dynamics of Dark Web communities: members come from worldwide; thus, they do not follow standard terminology or normative cultural context to contribute to the community.

Similarly, Queiroz and Keegan [4] indicated that hackers use constantly changing and evolving technical terms that contain semantic differences, in addition to abbreviations and misspellings, which require frequent development of the analysis model to keep pace with these changes. Moreover, it urges to adopt different modeling approaches for each social network; in other words, the model developed for a network may not perform similarly on another network due to terms changes. In another work, Queiroz et al. [57] justified the notion of "Concept Drift" caused by the mentioned changes in hackers' terms. Furthermore, they introduced an approach to overcome this drift by updating and retraining the model with temporal features and weighting.

Queiroz and Keegan [4] added two more challenges in the CTI field. One is the lack of ground-truth datasets that researchers need to evaluate their modeling approaches and validate their results. The second are the ethical considerations when dealing with the data. Unlike common social media platforms (such as Facebook and Twitter), there is no explicit agreement in hacking forums and chat rooms explaining to the user that their data may be used by third parties (such as researchers). Additionally, the sheer volume of data makes it difficult to obtain explicit consent for the use of participants' data in research. These considerations call for researchers to make careful decisions about how to use the acquired data.

In the technical particularity of the Dark Web, Akhgar et al. [58] addressed the following challenges:

(1) The nature of the web in general: the web consists of different types of media besides textual data, most commonly image, video, and audio.

(2) The published multimedia is in different languages and colloquialisms or accents, using different terminologies.

(3) The complexity of accessing criminals' social networks and closed groups: investigators often need to wait several weeks before obtaining approvals to join these networks. Moreover, they need to make their profiles look authentic, and their stories sound realistic and believable by administrators of the websites under study.

Due to the technical nature of the Dark Web, developing crawlers that collect and analyze the required data can be complicated. Furthermore, researchers must consider efficient precautionary measures since their employed techniques and tools themselves face the risk of being disclosed and vulnerable to cyberattacks [6].

In particular, Pastrana et al. [59] discussed the ethical issues when collecting and analyzing data from underground forums. Ethical considerations require research studies involving human participants to be reviewed by a Research Ethics Board (REB). The importance of such reviews is to consider the potential harm, how to reduce or avoid consequences, and protect the researchers from possible responsibilities.

Moreover, Pastrana et al. [59] differentiate ethical issues of collecting the data from analyzing the data. Their justification for this separation is due to the nature of each process. Collecting the data is to understand forum behavior as a computer system, whereas analyzing the data involves understanding human beings related to the collected data. In the former, researchers should consider some technical risks such as breaking terms of services of the platform or overcoming crawling prevention measures like CAPTCHAs. They suggest that if the benefits surpass the potential harms, it is ethically reasonable to break such measures. On the other hand, using TOR for research purposes cannot avoid making the researcher's device itself a relay on the network.

Researchers can consider several measures to mitigate potential harm [59]:

(1) Avoiding identification of individuals (such as publishing their usernames)

(2) Introducing the results objectively

(3) Avoiding the disclosure of sensitive personal data (like credit card numbers of victims)

(4) Protecting the researcher: for example, by avoiding making comments that offend the community and taking precautions not to download malicious content, which can cause security or legal issues, such as malware, child pornography, or terrorist materials

(5) Hiding the name of the platform from which the researcher collected and analyzed the data

(6) Taking cautions when analyzing leaked data, as it can include private messages, e-mail addresses, IP addresses, and exclusive posts

6. Discussion and Future Directions

Leukfeldt et al. [5] found that forums play a significant role in originating cybercriminal networks. Forums help individuals or small groups find colleagues for collaboration and encourage the growth of the networks. Therefore, it is advantageous to analyze Dark Web forums to discover how cybercriminals' networks originate and grow, and understand the factors that attract individuals and groups to be active on these forums [5].

In addition to SNA, researchers need to study the types of criminals who communicate with each other on Dark Web platforms, their technical expertise levels, and the number of attacks generated in discussions. Furthermore, it is imperative to understand whether members' participation in forums is only for the sake of curiosity, or they are petty

thieves, or whether they form a professional network that carries out organized crime on various organizations systematically [5].

Vilić [60] indicated another type of crime that can be categorized under cyber threats but on an extensively wide scale, which is Cyber Terrorism. Cyber Terrorism can take many forms, including Logic Bombs, Trojan horses, Worms, Viruses, and other cyberattacks. Such attacks target large systems of critical institutions in countries (such as air forces, transportations, hospitals, and others), causing these systems to shut down, malfunction, or lose information. Vilić [60] mentioned the diverse definitions of Cyber Terrorism, its various goals, and techniques, all of which can lead to more future research in several different directions. Similar to CTI, these directions include disclosing criminals' identities and their supporting entities, and acquiring information related to the attacks, such as tools, techniques, methods, targets, motivations, and when these attacks will occur.

One challenging aspect of Dark Web analysis, which has limited research, is analyzing the encrypted messages exchanged among forum members. Future CTI tools can obtain considerable benefit from identifying members that use these encrypted means of communication and the content of the messages that may comprise extremely vital information about future cyberattacks [60].

Moreover, future directions will involve extensive employment of Social Network Analysis, Content Analysis, Link Analysis, and Sentiment Analysis conducted on various platforms on the Dark Web. These techniques help understand attacks and attackers by identifying criminals and detecting attacks patterns, leading organizations to take the proper proactive measures against them [60].

From the linguistics perspective, few research studies exist in analyzing the Dark Web content in different languages. It is noteworthy that not all content of the Dark Web is in English; conversely, many other languages are heavily used in Dark Web platforms, singularly or in a multilingual way. This aspect needs further research.

Cyber Threat Intelligence and Cyber Terrorism detection can leverage an integrated analysis of the virtual criminal environment and the physical or conventional crime world. Such studies can lead to identifying the geographical location of attackers, as researchers suggest that some criminal networks may originate in the physical world before transferring them to the cyber world [5].

An emerging area of research is how to exchange CTI among security organizations via secure channels to extend the level of protection and responses against cyberattacks. However, cyberattacks are rapidly becoming more complex, more extensive, and more effective due to the wide variety of methods, technologies, and platforms used by cyber threat actors. Therefore, the CTI domain needs constant developments, particularly implementing appropriate real-time procedures, to keep pace with the level of attacks and threats [21].

In their review, Samtani et al. [13] suggested four directions for future development in the CTI industry domain:

(1) A genuine shift from developing reactive CTI tools to developing proactive OSINT-based CTI platforms

(2) Sufficient adoption of AI and ML techniques, such as NLP, text mining techniques, TM, ontology development, named-entity recognition (NER), and diachronic linguistics.

(3) The immense use of optimized DM methods

(4) The integration of Big Data and Cloud Computing technologies: Big Data tools help to extract features, reduce feature space, and improve the performance of DM methods. Moreover, Cloud Computing enables organizations to increase their capabilities by extending their operating environment across the Cloud.

More specifically, ontology techniques have a promising lead in the future of CTI. A multilayer CTI ontology can integrate formal definitions and lexicons, representing the abstract layer of CTI in ontology with defined constraints for the proper utilization of Web Ontology Language (OWL) capabilities [2].

On a different aspect, Saalbach addressed the process of Attribution, defining it as "the identification of the origin of a cyberattack" [61], which implies the identity of the attacker (individual or organization) as well, and it includes both the digital and physical worlds. In this context, Saalbach suggested integrating both cyber and conventional intelligence against cyberattack and their actors. Therefore, cooperation among organizations of different specialties is essential for successful attribution [61]. Moreover, matching cyberattack actors' identities among several platforms requires further research [6].

One crucial aspect, and in light of what we have discussed in this review, social relations among cybercriminals play a key role in executing large-scale cyberattacks and achieving their shared objectives (financial or nonfinancial). Such cooperation represents a type of organized crime or Crime-as-a-Service (CaaS). Therefore, it is advantageous to integrate computational modeling with social modeling to understand how these societies arise, develop, and grow, and eventually how they plan and perform organized attacks. Applying a Sociological Model of the Organizational Development of criminal networks helps to understand their structure, levels of professions or roles, their evolution over time, and their objectives [19].

7. Conclusion

With the rapid increase in quantity and complexity of cyber threats emerging from different parts of the Internet, organizations are increasingly considering Cyber Threat Intelligence (CTI) as one of the vital systems of their operational existence. CTI leverages multiple information sources and produces valuable insights, analytics, and knowledge for decision-makers to take proper actions against cyber threats. One of the most crucial sources is the Dark Web, which is growingly earning great interest from researchers due to its richness of information related to

cyber threats presented by cybercriminals on different sorts of platforms such as forums (discussions, tutorials, and assets) and marketplaces (offered products and services).

In this review, we discussed the particularity of the Dark Web as an information source for an effective CTI through several state-of-the-art research, whether including the Dark Web solely or combining it with other sources such as the Surface Web and Deep Web or shared information from cybersecurity institutions. We compared their goals, approaches, used methods and tools, case studies, results, and possible limitations to assist future researchers in acquiring the necessary information about CTI and Dark Web in particular and finding gaps that need further research. Furthermore, we discuss the critical challenges, ethical considerations, and future directions in this specific domain.

CTI in the future may, or should, witness more engagement of artificial intelligence, machine learning, language processing, and ontology techniques to respond proactively and promptly to the relentlessly evolving cyber threats, achieving at the same time high standards of accuracy, effectiveness, and efficiency. Although these countermeasures cannot completely extirpate the malicious parts of the web, they can extensively alleviate the severe effects of the threats lurking in those parts.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] W. Tounsi, "What is cyber threat intelligence and how is it evolving?," in *Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT*, W. Tounsi, Ed., ISTE Ltd, Washington, NJ, USA, 2019.

[2] A. Dutta and S. Kant, "An overview of cyber threat intelligence platform and role of artificial intelligence and machine learning," in *Proceedings of the 16th International Conference, ICISS 2020, Lecture Notes in Computer Science book series (LNCS)*, pp. 81–86, Jammu, India, December 2020.

[3] Z. Mador, "Keep the dark web close and your cyber security tighter," *Computer Fraud & Security*, vol. 2021, no. 1, pp. 6–8, 2021.

[4] A. L. Queiroz and B. Keegan, "Challenges of using machine learning algorithms for cybersecurity: a study of threat-classification models applied to social media communication data," in *Cyber Influence and Cognitive Threats*, J. M. Vladlena Benson, Ed., Academic Press, Elsevier Inc., Cambride, MA, USA, 2020.

[5] E. R. Leukfeldt, E. R. Kleemans, and W. P. Stol, "Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks," *British Journal of Criminology*, vol. 57, no. 3, pp. 704–722, 2017.

[6] P. Shakarian, "Dark-web cyber threat intelligence: from data to intelligence to prediction," *Information*, vol. 9, no. 12, p. 305, 2018.

[7] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & Security*, vol. 72, pp. 212–233, 2018.

[8] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: survey and research directions," *Computers & Security*, vol. 87, p. 101589, 2019.

[9] T. Miloshevska, "Dark web as a contemporary challenge to cyber security," *Kriminalističke Teme*, vol. 5, pp. 117–128, 2019.

[10] N. M. Chayal and N. P. Patel, "Review of machine learning and data mining methods to predict different cyberattacks," in *Data Science and Intelligent Applications, Proceedings of ICDSIA 2020*Springer, Gujarat, India, 2020.

[11] S. Samtani, M. Kantarcioglu, and H. Chen, "Trailblazing the artificial intelligence for cybersecurity discipline: a multi-disciplinary research roadmap," *ACM Transactions on Management Information Systems*, vol. 11, no. 4, pp. 1–19, 2020.

[12] R. Montasari, F. Carroll, S. Macdonald, H. Jahankhani, A. Hosseinian-Far, and A. Daneshkhah, "Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence," in *Digital Forensic Investigation of Internet of Things (IoT) Devices*, R. Montasari, H. Jahankhani, R. Hill, and S. Parkinson, Eds., Springer, Berlin, Germany, 2021.

[13] S. Samtani, M. Abate, V. Benjamin, and W. Li, "Cybersecurity as an industry: a cyber threat intelligence perspective," in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, T. J. Holt and A. M. Bossler, Eds., Palgrave Macmillan, London, USA, 2020.

[14] R. Liggett, J. R. Lee, A. L. Roddy, and M. A. Wallin, "The dark web as a platform for crime: an exploration of illicit drug, firearm, CSAM, and cybercrime markets," in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, T. J. Holt and A. M. Bossler, Eds., Palgrave Macmillan, London, UK, 2020.

[15] J. N. Pelton and I. B. Singh, "Coping with the dark web, cybercriminals and techno-terrorists in a smart city," in *Smart Cities of Today and Tomorrow-Better Technology*Cham, Massy, France, 2019.

[16] G. Hurlburt, "Shining light on the dark web," *Computer*, vol. 50, no. 4, pp. 100–105, 2017.

[17] A. Grimani, A. Gavine, and W. Moncur, "An evidence synthesis of strategies, enablers and barriers for keeping secrets online regarding the procurement and supply of illicit drugs," *International Journal of Drug Policy*, vol. 75, p. 102621, 2020.

[18] G. Me and L. Pesticcio, "Tor black markets: economics, characterization and investigation technique," in *Cyber Criminology. Advanced Sciences and Technologies for Security Applications*, H. Jahankhani, Ed., Springer, Berlin, Germany, 2018.

[19] E. R. Leukfeldt and T. J. Holt, "Examining the social organization practices of cybercriminals in The Netherlands online and offline," *International Journal of Offender Therapy and Comparative Criminology*, vol. 64, no. 5, pp. 522–538, 2020.

[20] O. Cherqi, G. Mezzour, M. Ghogho, and M. E. Koutbi, "Analysis of hacking related trade in the darkweb," in *Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Miami, FL, USA, November 2018.

[21] A. Sari, "Context-aware intelligent systems for fog computing environments for cyber-threat intelligence," in *Fog*

Computing: Concepts, Frameworks and Technologies, Z. Mahmood, Ed., Springer, Berlin, Gemany, 2018.

[22] I. Alsmadi, "Cyber intelligence," in *The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics*Springer, Berlin, Germay, 2019.

[23] P. Shakarian: The Enemy Has a Voice: Understanding Threats to Inform Smart Investment in Cyber Defense," 2021].

[24] A. Sapienza, A. Bessi, S. Damodaran, P. Shakarian, K. Lerman, and E. Ferrara, "Early warnings of cyber threats in online discussions," in *Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW)*, New Orleans, LA, USA, November 2017.

[25] M. Almukaynizi, E. Nunes, K. Dharaiya, M. Senguttuvan, J. Shakarian, and P. Shakarian, "Proactive identification of exploits in the wild through vulnerability mentions online," in *Proceedings of the 2017 International Conference on Cyber Conflict (CyCon U.S.)*, pp. 82–88, Washington, DC, USA, May 2017.

[26] M. Almukaynizi, E. Marin, E. Nunes et al., "DARKMENTION: a deployed system to predict enterprise-targeted external cyberattacks," in *Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 31–36, Miami, FL, USA, November 2018.

[27] R. Williams, S. Samtani, M. Patton, and H. Chen, "Incremental hacker forum exploit collection and classification for proactive cyber threat intelligence: an exploratory study," in *Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Miami, FL, USA, November 2018.

[28] S. Narayanan, A. Ganesan, K. Joshi, T. Oates, A. Joshi, and T. Finin, "Early detection of cybersecurity threats using collaborative cognition," in *Proceedings of the 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, pp. 354–363, Philadelphia, PA, USA, October 2018.

[29] N. Tavabi, P. Goyal, M. Almukaynizi, P. Shakarian, and K. Lerman, "DarkEmbed: exploit prediction with Neural Language models," in *Proceedings of the AAAI Conference on Artificial Intelligence*, pp. 7849–7854, New Orleans, LA, USA, February 2018.

[30] N. Arnold, M. Ebrahimi, N. Zhang et al., "Dark-net ecosystem cyber-threat intelligence (CTI) tool," in *Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 92–97, Shenzhen, China, March 2019.

[31] B. Ampel, S. Samtani, H. Zhu, S. Ullman, and H. Chen, "Labeling hacker exploits for proactive cyber threat intelligence: a deep transfer learning approach," in *Proceedings of the 2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 1–6, Arlington, VA, USA, November 2020.

[32] P. Koloveas, T. Chantzios, S. Alevizopoulou, S. Tryfonopoulos , and C. Tryfonopoulos, "INTIME: a machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence," *Electronics*, vol. 10, no. 7, p. 818, 2021.

[33] S. Samtani, R. Chinn, and H. Chen, "Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence," *Journal of Management Information Systems*, vol. 34, no. 4, pp. 1023–1053, 2017.

[34] J. Grisham, S. Samtani, M. Patton, and H. Chen, "Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence," in *Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 13–18, Beijing, China, November 2017.

[35] S. Pastrana, A. Hutchings, A. Caines, and P. Buttery, "Characterizing eve: analysing cybercrime actors in a large underground forum," in *Research in Attacks, Intrusions, and Defenses. RAID*Springer, Berlin, Germany, 2018.

[36] B. Biswas, A. Mukhopadhyay, and G. Gupta, ""Leadership in action: how top hackers behave": a big-data approach with text-mining and sentiment analysis," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 1752–1761, Big Island, HI, USA, January 2018.

[37] E. Marin, J. Shakarian, and P. Shakarian, "Mining key-hackers on darkweb forums," in *Proceedings of the 2018 1st International Conference on Data Intelligence and Security (ICDIS)*, pp. 73–80, South Padre Island, TX, USA, April 2018.

[38] E. Marin, M. Almukaynizi, E. Nunes, J. Shakarian, and P. Shakarian, "Predicting hacker adoption on darkweb forums using sequential rule mining," in *Proceedings of the 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications*, pp. 1183–1190, Melbourne, Australia, December 2018.

[39] A. Deb, K. Lerman, and E. Ferrara, "Predicting cyber-events by leveraging hacker sentiment," *Information*, vol. 9, no. 11, p. 280, 2018.

[40] A. Zenebe, M. Shumba, A. Carillo, and S. Cuenca, "Cyber threat discovery from dark web," in *Proceedings of the 28th International Conference on Software Engineering and Data Engineering*, Toulouse, France, October 2019.

[41] E. Marin, M. Almukaynizi, and P. Shakarian, "Reasoning about future cyber-attacks through socio-technical hacking information," in *Proceedings of the 2019 IEEE 31st International Conference on Tools with Artificial Intelligence (ICTAI)*, pp. 157–164, Portland, OR, USA, November 2019.

[42] S. Sarkar, M. Almukaynizi, J. Shakarian, and P. Shakarian, "Predicting enterprise cyber incidents using social network analysis on dark web hacker forums," in *Proceedings of the Cyber Defense Review*, pp. 87–102, SPECIAL EDITION: International Conference on Cyber Conflict (CYCON U.S.): Cyber Conflict During Competition, Washington, DC, USA, November 2018.

[43] C. Huang, Y. Guo, W. Guo, and Y. Li, "HackerRank: identifying key hackers in underground forums," *International Journal of Distributed Sensor Networks*, vol. 17, no. 5, p. 15501477211015145, 2021.

[44] I. Deliu, C. Leichter, and K. Franke, "Extracting cyber threat intelligence from hacker forums: support vector machines versus convolutional neural networks," in *Proceedings of the 2017 IEEE International Conference on Big Data (Big Data)*, pp. 3648–3656, Boston, MA, USA, December 2017.

[45] I. Deliu, C. Leichter, and K. Franke, "Collecting cyber threat intelligence from hacker forums via a two-stage, hybrid process using support vector machines and latent dirichlet allocation," in *Proceedings of the 2018 IEEE International Conference on Big Data (Big Data)*, pp. 5008–5013, Seattle, WA, USA, December 2018.

[46] P. Koloveas, T. Chantzios, C. Tryfonopoulos, and S. Skiadopoulos, "A crawler architecture for harvesting the clear, social, and dark web for IoT-related cyber-threat intelligence," in *Proceedings of the 2019 IEEE World Congress on Services*, pp. 3–8, Milan, Italy, July 2019.

[47] A. L. Queiroz, S. Mckeever, and B. Keegan, "Detecting hacker threats: performance of word and sentence embedding models in identifying hacker communications," in *Proceedings of the 27th AIAI Irish Conference on Artificial Intelligence*

and Cognitive Science AICS 2019, pp. 116–127, Galway, Ireland, December 2019.

[48] J. W. Johnsen and K. Franke, "The impact of preprocessing in natural language for open source intelligence and criminal investigation," in *Proceedings of the 2019 IEEE International Conference on Big Data (Big Data)*, pp. 4248–4254, Los Angeles, CA, USA, December 2019.

[49] M. Ebrahimi, J. F. Nunamaker, and H. Chen, "Semi-supervised cyber threat identification in dark net markets: a transductive and deep learning approach," *Journal of Management Information Systems*, vol. 37, no. 3, pp. 694–722, 2020.

[50] E. Nunes, P. Shakarian, and G. I. Simari, "At-risk system identification via analysis of discussions on the darkweb," in *Proceedings of the 2018 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–12, San Diego, CA, USA, May 2018.

[51] M. Ebrahimi, M. Surdeanu, S. Samtani, and H. Chen, "Detecting cyber threats in non-English dark net markets: a cross-lingual transfer learning approach," in *Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 85–90, Miami, FL, USA, November 2018.

[52] M. Schäfer, M. Fuchs, M. Strohmeier, M. Engel, M. Liechti, and V. Lenders, "BlackWidow: monitoring the dark web for cyber security information," in *Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon)*, pp. 1–21, Tallinn, Estonia, May 2019.

[53] M. Ebrahimi, S. Samtani, Y. Chai, and H. Chen, "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)*, pp. 20–26, San Francisco, CA, USA, May 2020.

[54] F. Dong, S. Yuan, H. Ou, and L. Liu, "New cyber threat discovery from darknet marketplaces," in *Proceedings of the 2018 IEEE Conference on Big Data and Analytics (ICBDA)*, pp. 62–67, Langkawi, Malaysia, November 2018.

[55] E. Marin, M. Almukaynizi, E. Nunes, and P. Shakarian, "Community finding of malware and exploit vendors on darkweb marketplaces," in *Proceedings of the 2018 1st International Conference on Data Intelligence and Security (ICDIS)*, pp. 81–84, South Padre Island, TX, USA, May 2018.

[56] R.-H. Ferguson, "Offline 'stranger' and online lurker: methods for an ethnography of illicit transactions on the darknet," *Qualitative Research*, vol. 17, no. 6, pp. 683–698, 2017.

[57] A. L. Queiroz, B. Keegan, and S. Mckeever, "Moving targets: addressing concept drift in supervised models for hacker communication detection," in *Proceedings of the 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pp. 1–7, Dublin, Ireland, June 2020.

[58] B. Akhgar, P. Bertrand, C. Chalanouli et al., "TENSOR: retrieval and analysis of heterogeneous online content for terrorist activity recognition," in *Proceedings of the Estonian Academy of Security Sciences, 16: From Research to Security Union*, Tallinn, Estonia, October 2017.

[59] S. Pastrana, D. R. Thomas, A. Hutchings, and R. Clayton, "CrimeBB: enabling cybercrime research on underground forums at scale," in *Proceedings of the Proceedings of the Web Conference 2018 (WWW 2018)*, pp. 1845–1854, Lyon, France, April 2018.

[60] V. M. Vilić, "Dark web, cyber terrorism and cyber warfare: dark side of the cyberspace," *Balkan Social Science Review*, vol. 10, no. 10, pp. 7–25, 2017.

[61] K.-P. Saalbach, "Attribution of cyber attacks," in *Information Technology for Peace and Security-IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*, C. Reuter, Ed., Springer Vieweg, Wiesbaden, Germany, 2019.