SAKARYA UNIVERSITY JOURNAL OF COMPUTER AND INFORMATION SCIENCES
VOL. 5, NO. 1, APRIL 2022
DOI: 10.35377/ saucis.05.01. 950746

Review Article

Terrorism in Cyberspace: A Critical Review of Dark Web Studies under the Terrorism Landscape

Eda Sonmez[1], Keziban Seckin Codal[2]
[1]Corresponding Author; Ankara Yildirim Beyazit University; Department of Management Information Systems; edasonmez@uludag.edu.tr; 03123230134
[2] Ankara Yıldırım Beyazıt University; Department of Management Information Systems; kseckin@ybu.edu.tr;

Received 10 June 2021; Revised 25 August 2021; Accepted 8 November 2021; Published online 30 April 2022

Abstract

Crime, terrorism, and other illegal activities are increasingly taking place in cyberspace. Crime in the dark web is one of the most critical challenges confronting governments around the world. Dark web makes it difficult to detect criminals and track activities, as it provides anonymity due to special tools such as TOR. Therefore, it has evolved into a platform that includes many illegal activities such as pornography, weapon trafficking, drug trafficking, fake documents, and more specially terrorism as in the context of this paper. Dark web studies are critical for designing successful counter-terrorism strategies. The aim of this research is to conduct a critical analysis of the literature and to demonstrate research efforts in dark web studies related to terrorism. According to result of the study, the scientific studies related to terrorism activities have been minimally conducted and the scientific methods used in detecting and combating them in dark web should be varied. Advanced artificial intelligence, image processing and classification by using machine learning, natural language processing methods, hash value analysis, and sock puppet techniques can be used to detect and predict terrorist incidents on the dark web.

Keywords: terrorism, cyberspace, dark web, deep web, anonymity

1. Introduction

In the twenty-first century, governments face a new security threats that has evolved as a result of globalization and the ever-accelerating pace of technological breakthroughs [1]. As technological advances intensify, abuse has also increased especially in cyberspace and traditional terrorist groups are increasingly expanding their activities into the cyberspace [2], [3]. The combination of cyberspace and terrorism has also revealed the concept of cyber terrorism. Following the 9/11 attacks, cyber terrorism became a prominent topic in security and terrorism discussions [4].

The increase of cyber terrorism reflects the Internet's rising popularity, the substantial number of malicious activities, and the development of sophisticated and high-tech dependent tools.Understanding the characteristics of Internet is the important step in dealing with the cyber terrorism. The internet has three different layers called surface web, deep web and dark web [5].

The Surface Web, called as a visible, indexable Web is a tier of the internet that is readily available to the general public [6]. Presently, there are roughly 4.66 billion Internet users and 5,54 billion indexed pages around the world [7], [8]. Since the late 1990s, terrorists have been active in the surface web and use various social media platforms such as YouTube, Twitter to communicate, recruit and propagate [9]. The surface web poses danger for terrorists due to easily followed; hence, terrorists have shifted their illegal activities to the deeper layer of the Internet, deep and dark web.

The deep web is a part of the internet that can't be reached by conventional search engines; it can only be searched through specific keywords and queries, and it is protected by safety precautions involving membership records, login IDs, passwords, and codes [10]. According to Bergman (2001), the most cited

researcher on the scale of the deep web, the deep web is 4,000-5,000 times larger than the surface web. The term "Dark Web" refers to a part of the deep web that is purposefully concealed and accessible only through specific software [11]. The best known special tool for accessing and surfing on the dark web is Onion Router (TOR) [12]. TOR is a free tool that uses the onion routing technique to provide anonymity [13]. It was originally developed to protect the classified data of the US Naval Research Laboratory, but it has since grown into an encryption tool for hiding users' activities and IP addresses [14]. Criminals come together on dark web platforms to perform illegal activities [15]. Pornography, gun trafficking, illegal drug trade, fake documents and counterfeit currency, and terrorism cover 57% of the dark web crime [16].

Terrorist activities can be carried out directly over the dark web, at the same time, the other dark web crimes can also aid in the spread of terrorism. Terrorist groups also widely conduct illegal actions such as weapons trade, drug trafficking, human smuggling, money laundering, to provide resources and finance for their organizations. Thus, other dark web crimes also become an element of terrorism [17]. Dark web terrorism is a worldwide problem that requires multilateral effort at the national, regional and global levels [18]. The researchers and law enforcement has tended to focus upon the variety of illicit activities in the dark web to examine and determine the necessary precautions. It is vital to consider existing research specifically related to the dark web terrorism in order to address how cyber environments are used for terrorist acts. The aim of this paper is to critically review current studies as well as to summarize research efforts in the dark web in the scope of terrorism.

The rest of the paper structured as follows: The next section discusses the dark web in pertaining to terrorism. Evaluating and justifying the methodological choices are explained in Section 3. Results and discussions are presented in section 4 and finally, there is the conclusion part in section 5.

2. Terrorism and the Dark Web

Terrorism is typically described as violence that is designed to cause fear, is carried out for political, religious, or ideological purposes, intentionally ignore the protection of civilians. However, it does not have a generally accepted legal definition in the international area [19].

Terrorism damages stability and peace, creates violence in society and directly endangers the lives of people [20]. Due to terrorist attacks, the millions of innocent people are harmed, animals are also killed and millions of things are destroyed. The total number of deaths caused by terrorism between 2006 and 2019 is presented in Figure 1. The highest number of deaths was observed in 2014 and 2018. Additionally, it is noteworthy that the number of deaths has fluctuated in recent years.

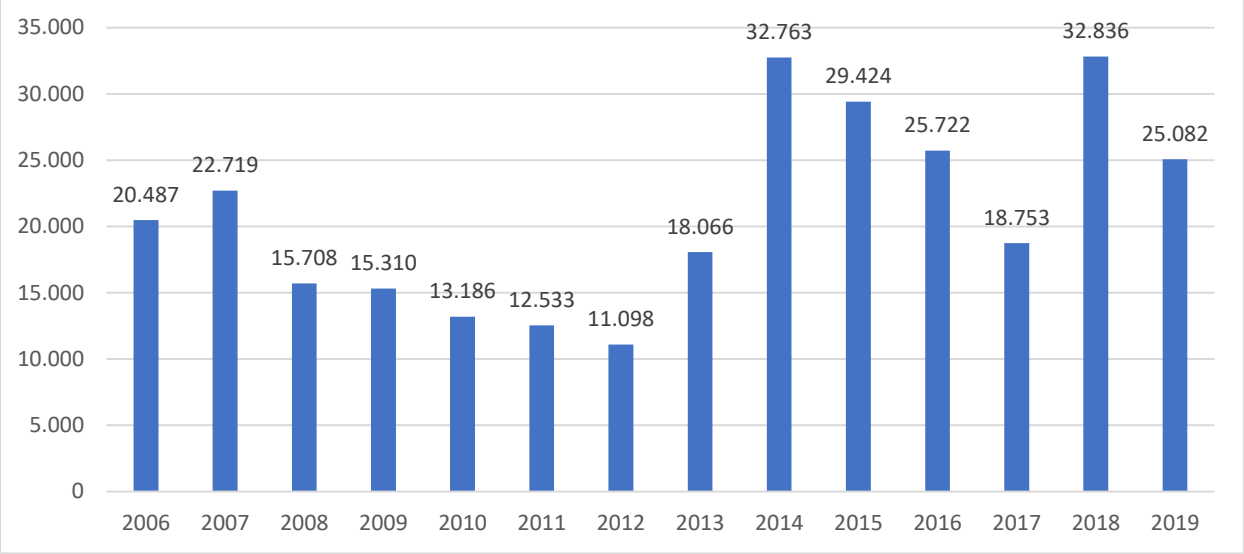

Figure 1 The total number of deaths caused by terrorism worldwide [21]

Moreover, terrorist incidents pose a serious threat to economic growth by damaging investment, tourism and consumption [22]. Targeting visitors and travel destinations, terrorism activities are one of the important factors that negatively affect the economy. The fear and anxiety created by terrorist attacks that harm public spaces and civilian population in particular lead to the loss of tourists, which is an important source of employment and currency in the economy [23]. The rates of foreign direct investment and portfolio investment have a very important share in economic development. However, companies and investors invest in countries where prosperity and security are developed, rather than in regions with high terrorism risk [24].

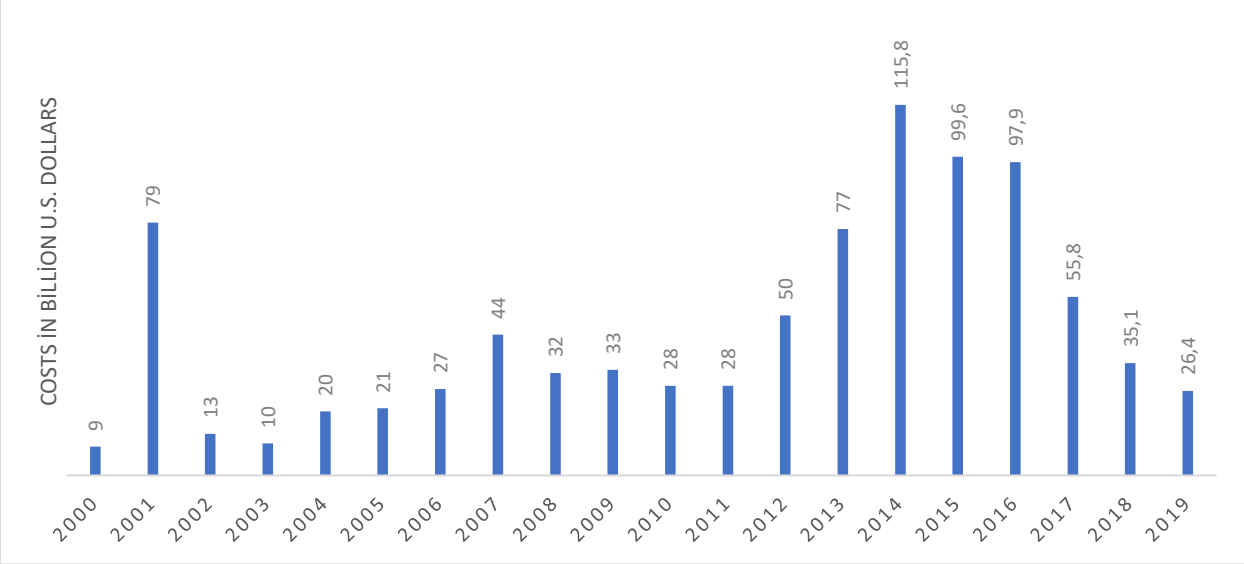

Figure 2 Global economic costs of terrorism 2000-2019 [19]

According to the Figure 2, terrorism cost totaled $ 901.6 billion between 2000 and 2019. The highest economic costs, at 115.8 billion dollars, were recorded in 2014. It has been observed that the cost of terrorism has decreased since 2014. The September 11, 2001 attacks is one of the most damaging terrorist incidents to the economy with $ 40.6 billion. The second most costly terrorist attack, the Sinjar massacre,

which resulted in the deaths of 104 members of the Yazidi community in Iraq by Islamic State groups in 2014, caused 104 million losses [22], [25].

Terrorist groups are global threats to the defense, infrastructure, and people of countries and communities around the world [26]. The most deadly terrorist groups in 2019 were the Taliban, Boko Haram, ISIL, and Al-Shabaab. They were responsible for 7.578 terrorism-related deaths in 2019, accounting for 55% of all terrorism-related deaths based on historical record [27].

Having no accepted universally definition [28], cybercrime is crimes that involve the use of a computer and hardware devices or network systems to inflict the vulnerable targets [29]. The computer or device can be the target as a perpetrator or facilitator, as well as the crime can be committed in other non-virtual places. Therefore, cybercrime can be classified into two different types. The first type of cybercrime is usually singular incidents from the perspective of the victim and it is more technical nature. It occurs when criminal software programs such as viruses, trojans, etc., infiltrate the user's computer through security vulnerabilities. The second type of cybercrime, on the other hand, usually involves repeated contacts or events from the user's point of view, and is often facilitated by programs that do not fit into the crimeware classification, such as instant messaging. Cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation, intricate corporate espionage, and planning or carrying out terrorist actions online are all examples of the second type of cybercrime [30]. As seen in Table 1, there are various types of cybercrime. In this study, cyberterrorism will be examined in detail.

Table 1 The characteristics of cyber crimes [30]

Cybercrimes	**Type**	**Software**
Phishing	I	Mail Client
Identity Theft	I	Keylogger, Trojan
Cyberstalking	II	Email Client, Messenger Clients
DDoS	I	Bots
Cyberterrorism (communication)	II	Steganography, Encryption, Chat Software

Cyber terrorism was primarily defined as a planned attack on data and computer systems by terrorists. All kinds of terrorist activities that use Internet as a tool are covered in the concept of cyber terrorism [31]. Phishing, identity theft, cyber stalking, DDoS, cyberterrorism (communication) have been successfully committed through the Internet and also substantially affected with each other.

The globalization and modern technology have strengthened the presence of terrorists in cyberspace as well as physical environments [32]. In the 1990s, terrorists were used Internet for only cyber attacks in order to damage critical infrastructures. Subsequently, their purpose changed with the 9/11 attacks and they use the Internet mainly for propaganda, data mining, operations coordination, recruiting and fundraising [33]. Indeed, the perpetrators of the 9/11 attacks frequently contacted al-Qaeda leaders over the Internet to plan their attacks [34], [35].

On the surface web, counterterrorism teams can detect terrorist activities or remove extremist contents. These interventions have led terrorist groups to escape repression and move towards more anonymous environments that are difficult to monitor and identify [5]. Beatrice Berton from the European Union Security Institute stated that ISIS tend to employ new safe online environments due to government interventions on jihadists' extremist content on the Internet [14].

The anonymity provided by the dark web enables encryption for communication, additionally, cryptocurrencies provide privacy in the financial environment for terrorist activities [17]. Donors secretly fund terrorist group [36] and terrorists collect donations by taking advantage of the anonymity of cryptocurrencies on the dark web [37].

There is a lot of evidence that terrorists operate on the dark web. The French Interior Minister Bernard Cazeneuve stated that the terrorist organizations responsible for terrorist attacks in Europe through communicate using dark web (Weimann, 2015). The research conducted by The Institute for National Security Studies (INSS) (2013), Al-Qaeda is also one of the terrorist groups communicating over the dark web. In 2015, after the closure of many websites of ISIS in the Operation Paris (OpParis), the information required for the transition to the Dark Web was published in the Al-Hayat Media Center (ISIS media) and ISIS officially proclaimed that it would continue its activities on the dark web [5]. Terrorists publish the books and manuals about the use of the dark web and TOR for their supporters [39], [40]. In addition to establishing connections, ISIS members are also using dark web marketplaces to obtain fake IDs and passports as legal regulations increase in border controls [14]. Terrorist organizations such as Aum Shinrikyo and Al-Qaeda are experimenting with various methods for access to adequate and efficient resources, equipment, and qualified experts in order to produce chemical, biological, radiological, and nuclear (CBRN) weapons [41]. In order to acquire CBRN weapons, terrorists utilize the Dark Web as a source. They purchase materials of these weapons from the darknet markets and they recruit chemists or other staff knowledgeable about CBRN weapons production [42]. Even more terrifying, there is strong evidence that the weapons used in the 2015 Paris attacks and 2016 Munich attack were supplied from the dark web [43], [44].

Terrorism in cyberspace is an important issue that needs to be investigated and prevented, as it is cheaper, more anonymous, more universal, and more effective than "offline" terror. Throughout one computer and necessary software, terrorist ideas and propaganda can easily be transported across borders, more supporters can be found, and then innocent people is affected due to terrorist acts in the dark web [45]. Therefore, to mitigate these wide-ranging effects, national and international efforts should be stepped up to tackle terrorism in the cyber environment.

3. Research Methodology

The study aims to observe research efforts, detect the methodological gaps and gain further research opportunity of the dark web studies under the terrorism concept.

Our research questions (RQs) are;

RQ1: What is the main focus of the researchers?

RQ2: What types of data source are used to uncover criminals on the Dark Web?

RQ3: What systematic methods are implemented for detecting dark web crimes?

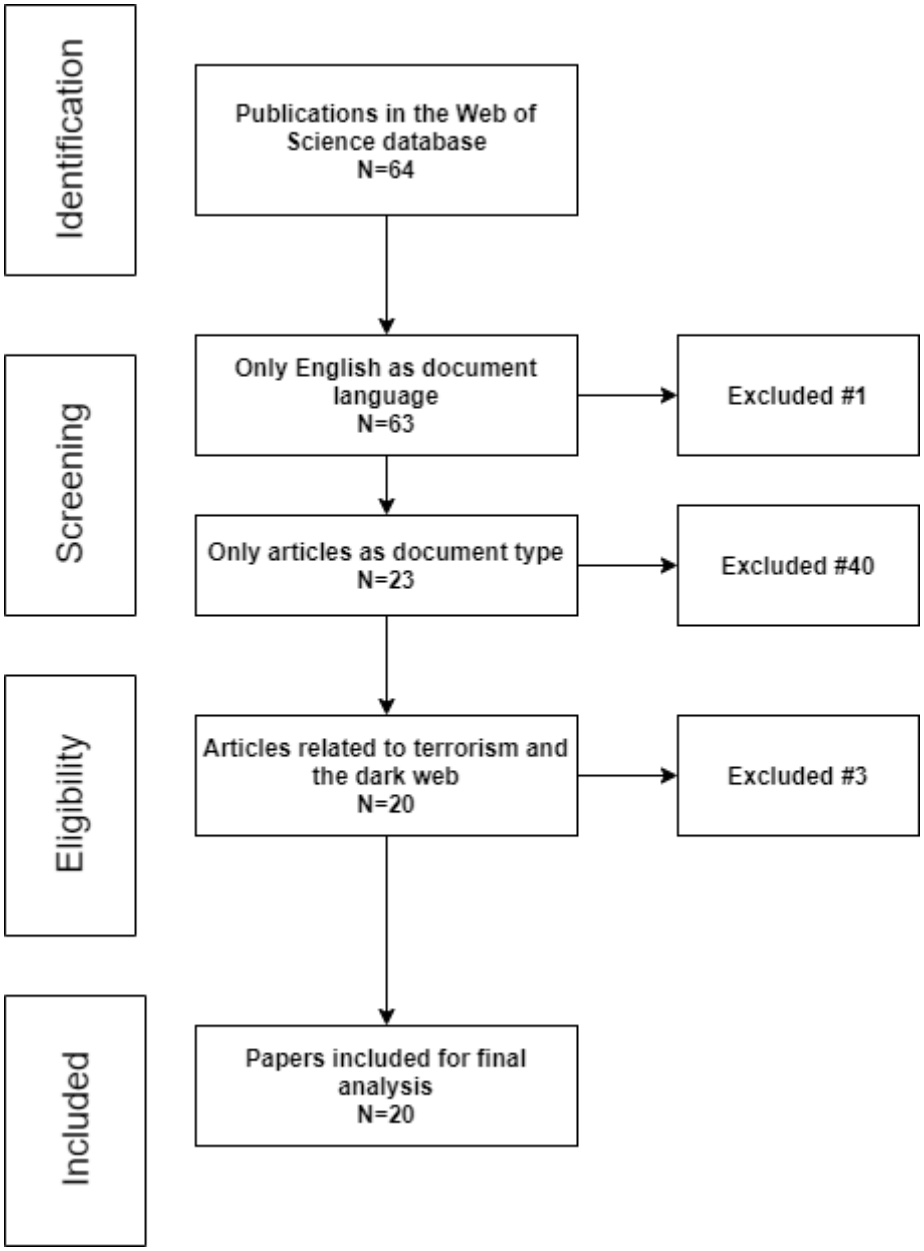

Figure 3 The flow diagram for the database search of publications for literature review

To address the research questions, a critical literature review method are applied to dark web studies within the scope of terrorism. A critical literature review is the assessment and overview of the ideas and information in manuscripts. There are two main points in critical review. The first is to scan the relevant literature efficiently and the second is to evaluate the information in the documents. Moreover, the content and different components of the text are analyzed. These components can define method that has boundaries such as the main theme of the text, data source, discussions made by the author and so on.

The flow diagram for the database search for publications is given in Figure 3. Web of science was chosen as the database since it is the world's most trusted publisher-independent global citation database. It is also a comprehensive platform with over 171 million records and 1.9 billion cited reference[46]. To collect data for the review articles, the most relevant keywords were selected. The search keywords were (("dark web"

OR "TOR" OR "anonymous network" OR "darknet") AND ("terrorism" OR "terrorist groups" OR "terrorist organization" OR "terrorist" OR "ISIL" OR "ISIS" OR "Daesh" OR "The Islamic State of Iraq and the Levant" OR "Al-Qaeda" OR "Boko Haram" OR "Taliban" OR "jihad" OR "jihadist" OR "cyberterrorism" OR "international security" OR "international terrorism")).

There were some searching criteria. There is no date and category limitation and only articles were selected as the document type, and only English was chosen as the studies' language as seen in Figure 3. As a result of searching, 23 studies were reached, but since three studies were found to be irrelevant to the topic, 20 studies were examined finally.

4. Result and Discussion

Determining the purposes of dark web studies under terrorism concept can be a clue for identifying emerging dark web threats and the focal points of acts. The foci, methods and data sources used to detect terrorist activities in the dark web studies will provide guide book to researchers with an overview of the latest methodologies used in combating dark web terrorism. The findings of the study are categorized in three different tables based on research design. Table 2 shows the detail of studies using quantitative research design, Table 3 figures the studies using qualitative research design, and also Table 4 represents the studies using mix research design.

According to Table 2, the motivations of studies using quantitative research were generally oriented identifying dark web contents, suggesting methods to determine crime pattern, detecting terrorist activities, and uncovering the illegal activities. In these studies, researchers generally collected the data in Dark websites which are primary data. Most of the studies using primary data are collaborative research. The co-authors may devote more resources and effort to data collection and analysis.

Table 2 The details of studies using Quantitative research design

Name	Year	Purpose	Data Types	Dataset	Data Source	Sample Size	Data Period	Data analysis method
[47]	2005	Discovery and analysis of the Dark Web content	Primary Data	Multimedia and multilingual Web contents	Dark Web	Not reported	until April 2004	The content and link analysis
[48]	2006	Suggesting a method for collecting Dark Web content and investigating terrorists' use of the Internet.	Primary Data	Multimedia Web documents	Dark Web	200.000 websites	until June 2004	Content Analysis
[49]	2006	Performing topological analyses of terrorist websites from various geographical region	Primary Data	Websites contents	Dark Web	311 Websites	until November 2004	Social network analysis
[35]	2007	Recommending an approach for collecting terrorist/extremist Web content on the Dark Web	Primary Data	Multimedia Web documents	Dark Web	200.000 Websites	until June 2004	Content Analysis
[50]	2015	Predicting the daily amount of violent extremist groups' cyber-recruitment activity	Secondary Data	Ansar1 forum posts	Dark Web Forum Portal	28.747 posts	December 2008- January - 2010	LDA and time series analysis
[51]	2016	Offering a hybridized term-weighting strategy for the detection of terrorist activities	Secondary Data	Arabic dark web pages and non- dark web pages	Dark Web Forum Portal and Open Source Arabic Corpora	1.000 Arabic dark web pages and non- dark web page	Not reported	Classification methods
[52]	2018	Examining internet users' views and perceptions about online hate speech and informing internet users and policy makers about cyberhate	Primary Data	Responses from survey participants	Internet users in Turkey and the USA	372 respondents	Not accessible	Survey

Table 2 The details of studies using Quantitative research design (continue)

[53]	2018	Examining the Tor structure and designing a strategy for quickly identifying places that may contain material of interest to law enforcement.	Primary Data	Website contents	Dark Web	232.792 sites	12 April 2016 -01 July 2016	Classification methods
[54]	2019	Developing automatic purchasing models to detect unauthorized firearm purchases by gathering and data from different discussion forums in the dark web	Secondary Data	Ansar Aljihad Network, Islamic Awakening,Gawaher,and Islamic Network forum sites	Dark Web Forum Portal	4,297,961 messages, 1,553,122 thread in the forums	2004-2012	Machine learning classification techniques (SVM, Boosting, Random Forest, GLMNET, Tree, and MAXEN)
[55]	2019	Creating a model that predicts a terrorist group's future lethality	Secondary Data	Information related to terrorist attacks	GTD and RAND	157 Terrorist Attacks	GTD-1970-2014 RAND-1968-2009	Regression analysis and simulation
[56]	2021	Proposing a link-based ranking approach for evaluating and identifying the hidden services in the Tor	Primary Data	Website contents	Dark Web	Not reported	Not reported	Link analysis

Qualitative research usually maintains the information about Dark web and terrorist activities as seen in Table 3. Some topics seem unrelated to terrorism such as Captagon -a psychostimulant drug- , animal trade, digital artifacts, however they are indirectly feed terrorism. Most of studies in qualitative research do not include method section and data sources. The methods section outlines included the research problem, specific procedures, process, and analysis of data relevant to understanding the problem provide the reader to critically assess the study's reliability and validity [57]. Therefore, the absence of a method section in these articles adversely affects the evaluation process. Table 3 displays all of the qualitative analysis using secondary data. Researchers focus on the literature, scientific publications, and various databases as data sources and the documentary analysis/review method is the main approach in qualitative research.

Table 3 The details of studies using Qualitative research design

Article	Year	Purpose	Data Types	Dataset	Data Source	Sample Size	Data Period	Data analysis method
[58]	2015	Examining studies that describe online data mining literature with a clear focus on law enforcement applications	Secondary Data	Scientific literature	IEEExplore, The ACM Digital Library, Springer-Link, ScienceDirect	206 publication	December 2012 - January 2013	Systematic literature review
[59]	2016	Presenting an overview of the most common darknets and their related information and the perspective of Law Enforcement Agencies on Open Source Intelligence	Secondary Data	Documents and scientific publications	Literature	Not reported	Not reported	Documentary analysis / Review and Case Study
[33]	2016	Presenting general information about the dark web and dark web terrorist activity.	Secondary Data	Documents and scientific publications	Literature	Not reported	Not reported	Documentary analysis / Review
[60]	2016	Providing detailed information on wildlife smuggling via the dark web, as well as a map of the trafficking of animal parts	Secondary Data	Documents and scientific publications	Literature	Not reported	Not reported	Documentary analysis / Review
[61]	2016	Getting the most up-to-date information on Captagon e-commerce in the Middle East	Secondary Data	Websites, drug forums and other online resources in both English and Arabic, literature	Medical and paramedical databases, web ,Darkweb, and the Global Public Health Intelligence Network database	Not reported	October 2015- May 2016	Thematic analysis
[62]	2018	Investigating Dark Web networks that exploit digital artifacts and identify the hidden actors behind these operations	Secondary Data	Documents and scientific publications	Literature	Not reported	Not reported	Document analysis / Review
[63]	2019	Defining the risks posed by the use of Fentanyl and Fentanyl +, as well as the demographic at risk.	Secondary Data	Documents and scientific publications	Literature	Not reported	Not reported	Documentary analysis / Review

While many studies in the cyber terrorism literature addressed the quantitative and qualitative research design, two studies used mixed research design as seen in Table 4. They compile both data types and have sophisticated data analysis methods.

Table 4 The details of studies using mixed research design

Article	**Year**	**Purpose**	**Data Types**	**Dataset**	**Data Source**	**Sample Size**	**Data period**	**Data analysis method**
[64]	2008	Creating a modern approach to gathering and analyzing Dark Web data.	Primary Data	Web sites contents	Dark Web	94. 326 websites	until 2004	Web page clustering, classification, and case study
[65]	2011	Offering an explanation about new phenomenon called as "Terrorism Informatics"	Primary and Secondary Data	Books, terrorism research centers and resources, and international terrorist organizations	Think Tanks and Intelligence Resources, Terrorism Databases and Online Resources, Higher Education Research Institutes, and the Dark Web	10.000 website, 300 terrorist forums in the Dark Web	Not reported	Review, Social Network Analysis, Content Analysis, Web Metric Analysis, Sentiment and Affect Analysis, Authorship Analysis and Writeprint, Video Analysis

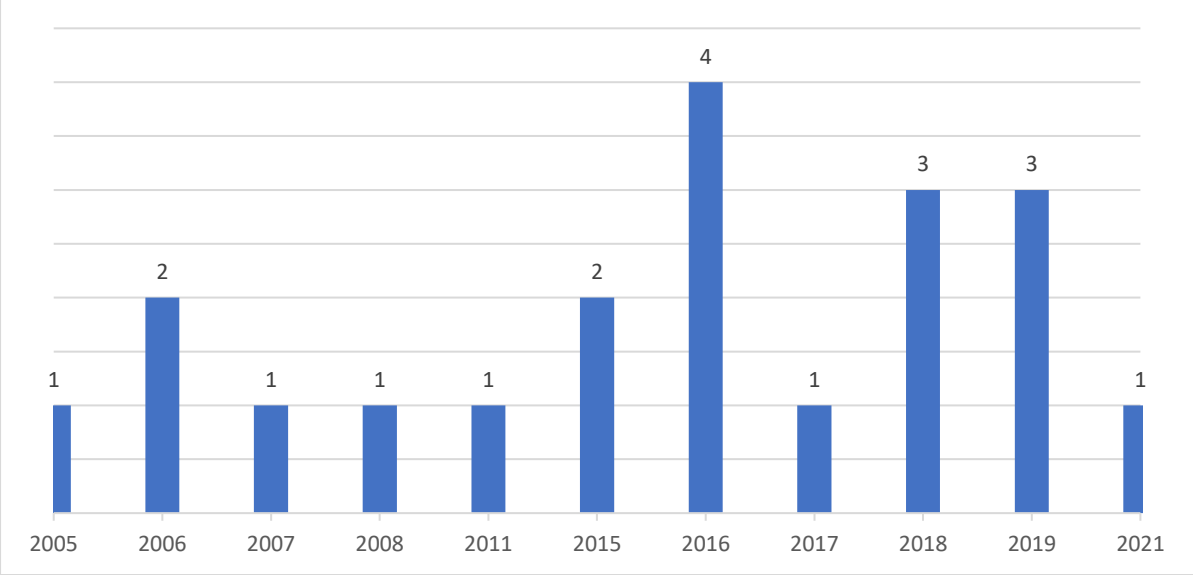

Figure 4 Period of published articles

Consequently, the number of studies is quite insufficient but these are still important topics. Although, there was no time and research area limitation, the interest and study efforts in this field are inadequate. As seen in Figure 4, the number of publications is excessive as an instance in 2016, 2018 and 2019 compare with the other timespan, there are no publications before 2005. The first use of the Dark Web phrase dates back to the 2000s [66], and also the first scientific study on terrorism activities in the dark web was published in 2005. A few articles were published in most years, and nearly 50% of the total publications were published in 2016, 2018 and 2019. In addition, there are no manuscripts in 2009, from 2012 to 2014 and in 2020 as well. This indicates that there is an academic gap in this field. The same authors mostly have their manuscripts since 2011. The articles [36] and [49] are the same in terms of purpose, dataset and method, but they have published as different articles.

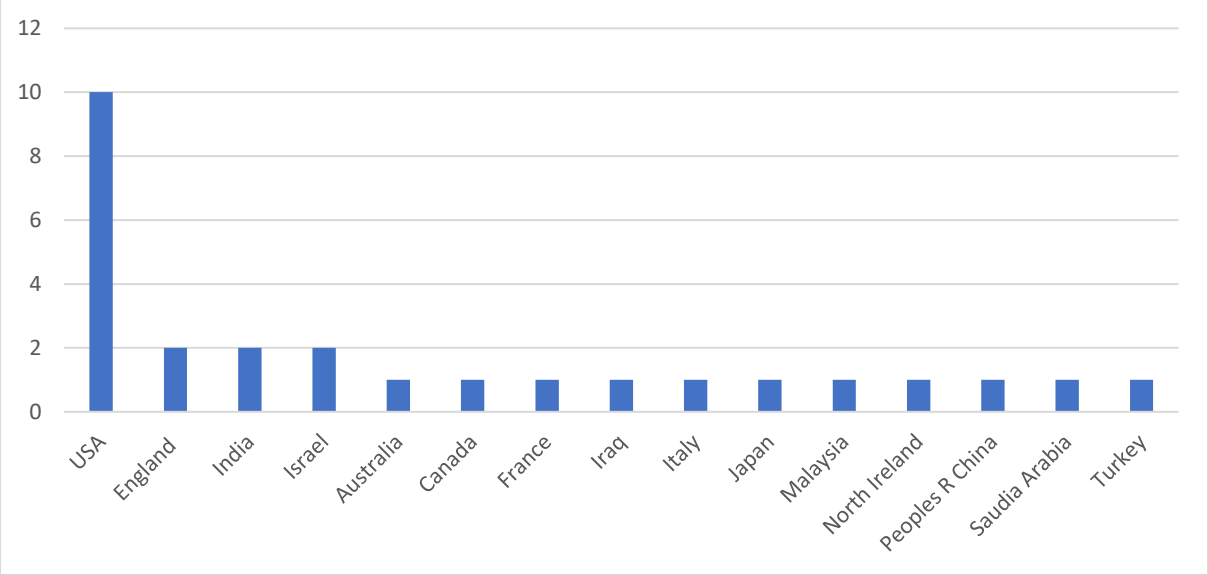

Figure 5 The distribution of articles by region

The majority of studies are from the United States, followed by England, India and Israel according to Figure 5. USA is one of the countries with the highest dark web usage [67], and accordingly, most of the studies

originated from the USA. Turkey, however, despite being among the countries with the highest usage of dark web, it is surprising that there is lack of the dark web studies in the context of terrorism. Therefore, researchers' efforts in this field should increase in Turkey.

Approximately 38% of the studies were supported by funding agencies. This rate may be a reason for the limited number of studies. Without funding, researchers are more reluctant to innovative approaches and may have to redirect their research areas to other activities that require less resources, time, and effort [68].

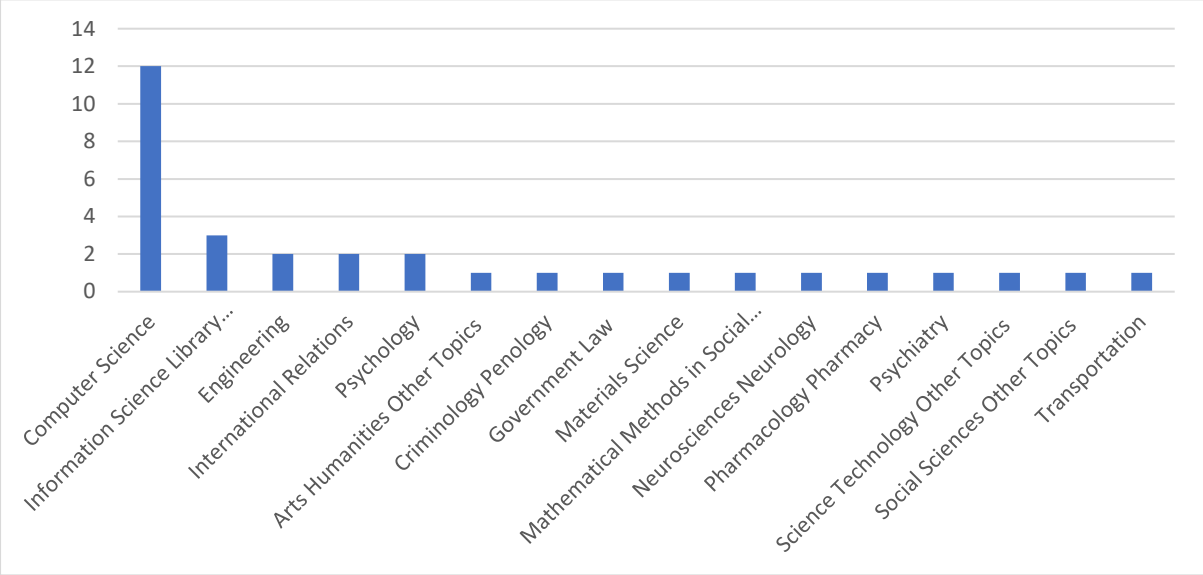

Figure 6 The distribution of articles according to web of science categories

The studies are concentrated in the category of Computer Science as seen in Figure 6. A little manuscript is in the international relations and social sciences interdisciplinary areas. Such research should be expanded in sociopolitical disciplines, as the topic also covers the notion of terrorism.

Researchers focus on providing a framework for understanding the concept of terrorism on the dark web and trying to identify trends and patterns in that concept. They frequently use descriptive analysis to learn general information about dark web and its components, comprehend structural characteristics, investigate terrorist incidents on the dark web, and establish the location of terrorist groups. They also utilized predictive analysis to make predictions about the future terrorist activities in the dark web.

The development of scientific approaches to explain and combat violent extremism is of worldwide interest [69]. The U.S. government alone spends half a trillion dollars every year investigating, fighting and reacting terrorism [70]. In terms of quantity, qualitative and quantitative methods utilized in dark web literature in the context of terrorism are comparable, but quantitative methods have a minor edge.

The principal methods of quantitative research performed on the dark web are social network analysis, link analysis and content analysis as seen in Table 2. Social network analysis is a method that uses various modeling techniques to examine the dynamics of social networks based on structure and interaction of communities [71]. In terrorist investigations, text mining techniques and social network analysis aid in the development of counter-terrorism approaches. Social network analysis can be useful for identifying key members of terrorist organizations, centrality measures for terrorism network, sub-groups detection, and so on [72].

The link analysis is known as the act of establishing networks of interconnected objects through relationships for discovering patterns and trends. It is commonly used to find central players and noteworthy patterns in dataset [73]. It is an effective method that can be used in dark web studies to destabilize the organization's activities by capturing some key figures in terrorist groups.

Analyzing the structure of terrorist networks can provide a technical understanding that can be used to prevent unlawful operations on the dark web [72]. Content analysis can be qualitative and quantitative techniques. The quantitative content analysis based on counting and measuring while qualitative content analysis based on interpreting and comprehending [74]. Quantitative content analysis is commonly used approach in dark web research to characterize the appearance of a variety of features in content, such as technical sophistication, media richness, and web interaction.

Classification methods are relatively implemented methods in dark web studies. The widespread term weighting methods, TF, DF, TF-IDF, Entropy and Glasgow are used to create structured data then analyze the web page. Many different effective techniques such as affect analysis, sentiment analysis, authorship analysis, latent Dirichlet allocation (LDA) were also applied. The sentiment and affect analysis allow for the identification of violent and extremist sites that pose serious threats [75]. The affect analysis of terrorists on the Dark Web reveals the dissemination of terror, hatred, and propaganda [72]. Another method, authorship analysis includes techniques for investigating the attributes of study in order to present conclusions on its authors [76]. Authorship analysis techniques are needed in cyber forensic to detect criminals on the Dark web who use services like TOR [72]. Topic based approach, LDA uncovers hidden topics from large document of corpus [77], and it can be used for specifying the topics discussed in the dark web.

Researchers tend to design research based on available data rather than collecting the data themselves. Because terrorists may disguise their identities and remove traces of their Internet actions, researchers and scholars have a tough time acquiring and analyzing Dark Web [64]. Other barriers of the collection are information overload and language barriers [78]. Therefore, researchers generally use secondary data instead of collecting their own dataset. The initial research relied on primary data due to young concept and the scarcity of secondary data. Spiders were used by the researchers to find the relevant terrorist groups based on reports from authoritative sources. The Dark Web Forum Portal (DWFP), which was created by collecting Dark Websites in 2004, was often used as a secondary dataset in later studies. The DWFP allows users to access vital foreign jihadist web forums through the Internet [79]. The forum sites named Gawaher, Islamic Awakening, Islamic Network, and Turn to Islam are closer to jihadist approaches, some studies used these forum sites' contents as data. The Global Terrorism Database (GTD) and RAND Database on World-wide Terrorism Incidents (RAND) are another databases referenced. Some studies is not depicted the time interval of data collection, so it is unclear whether the studies yield up-to-date results.

Future studies will require advanced analytical methodologies and terrorism databases or data collection methods to emerge complex interactions and activities in the Dark Web. Scholars should adapt a wider range of data collection techniques. Increased utilization of primary data could help researchers build a more solid empirical foundation for understanding terrorism and counterterrorism. They can create automated approaches that scrape the dark web with web scraping techniques for produced content assisted lawmakers and law enforcement [72]. Moreover, advanced artificial intelligence techniques, image processing, and natural language processing techniques, hash value analysis, sock puppet detection techniques can be applied as well. Advanced artificial intelligence techniques can be quite effective for tracking and detecting malicious activities. Image classification is one of the effective methods to detect unwanted, harmful or criminal content on Web pages. Detecting people who have criminal tendency by analyzing posts on Dark Web forums can be provided with natural language processing methods. Hash value analysis is a strong technique in cryptography for proving the authenticity of digital evidence during an inquiry [72]. The connecting server's destination can be determined via hash value analysis at the onion routing's exit node layer [80], [81]. Sock puppet is the use of numerous usernames or fake identity to converse online [82]. Sock puppet detection plays a critical role in monitoring communication and screening in the Dark Web for terrorist tracking [72].

5. Conclusion

This research identifies the existing research on dark web in the scope of terrorism and these studies are critically reviewed in terms of purpose, dataset, and applied method for identifying the criminals and crimes in the Dark Web.

According to the findings, the number of dark web research on terrorism was insufficient, indicating a gap in the literature. Thus, scholars and practitioners must continue to urge action in order to close the gap. The link analysis, web mining techniques, classification methods, affect analysis, sentiment analysis, authorship analysis, content analysis, and natural language processing techniques, documentary analysis/review are used in these studies. The dark web' anonymity gives drawback to discover crimes; hence, systematic methods for detection should be expanded. Advanced artificial intelligence, machine learning, deep learning, image processing, natural language processing techniques, hash value analysis, sock puppet detection techniques can be used to track and combat cyber-terrorism.

This study appears as one of the first papers that have mapped the literature exploring dark web studies in the scope of terrorism. New methods suggestions for improving dark web studies are offered through an overview of the academic publications. This constitutes a guideline for researchers and practitioners in the dark web field in the future. By using the critical review of existing literature, researchers can improve studies with new proposed methods and also contribute to the quantitative and qualitative research design in dark web studies, which are few in number.

This paper is limited by language restrictions. The only language of the reviewed studies was English. Moreover, only the Web of Science was used as a database. Another limitation is the low number of dark web studies in the context of terrorism. Sophisticated techniques to detect the main topics could not be used due to the scarcity of studies. Additionally, the lack of some details in some studies (areas indicated by "not reported" in table 2,3,4) is another point that challenges us during the analysis phase.

Future studies may focus on various databases, languages, and keywords to achieve more global results. The terrorism in the dark web can be examined with more advanced methods. Therefore, various text mining techniques, bibliometric analysis, and topic modeling approaches such as LDA can be applied on extensive literature. Furthermore, other evaluation criteria can be added in order to reach more comprehensive results.

References

[1] S. D. Keene, “Terrorism and the internet : a double-edged sword,” J. Money Laund. Control, vol. 14, no. 4, pp. 359–370, Oct. 2011, doi: 10.1108/13685201111173839.

[2] J. R. C. Nurse and M. Bada, “The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations,” Jan. 2019, doi: 10.1093/oxfordhb/9780198812746.013.36.

[3] D. Bieda and L. Halawi, “Cyberspace: A Venue for Terrorism,” 2015. Accessed: May 28, 2021. [Online]. Available: https://commons.erau.edu/publication/304.

[4] G. Weimann, “Cyberterrorism How Real Is the Threat?,” 2004. Accessed: May 28, 2021. [Online]. Available: www.usip.org.

[5] G. Weimann, “Going Darker ? The Challenge of Dark Net Terrorism,” 2015.

[6] M. Chertoff and T. Simon, “The Impact of the Dark Web on Internet Governance and Cyber Security,” Glob. Comm. Internet Govrnance, no. 6, pp. 6–8, 2015, [Online]. Available:

https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

[7] Statista, “Internet users in the world,” 2021. https://www.statista.com/statistics/617136/digital-population-worldwide/ (accessed Dec. 22, 2020).

[8] M. de Kunder, “The size of the World Wide Web (The Internet),” 2020. https://www.worldwidewebsize.com/ (accessed Dec. 21, 2020).

[9] G. Weimann, “Terrorist Migration to the Dark Web,” Perspect. Terror., vol. 10, no. 3, pp. 40–44, 2016.

[10] M. . Bergman, “The deep Web: Surfacing hidden value,” J. Electron., vol. 7, no. 1, 2001.

[11] K. Finklea, “Dark Web,” Taylor and Francis Inc., Mar. 2017. doi: 10.1080/1057610X.2015.1119546.

[12] E. Jardine, “The Dark Web Dilemma: Tor, Anonymity and Online Policing,” 2015. Accessed: Jan. 21, 2021. [Online]. Available: https://ssrn.com/abstract=2667711.

[13] R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The Second-Generation Onion Router,” 2004.

[14] B. Berton, “The dark side of the web : ISIL ’ s one-stop shop ?,” no. June, pp. 1–2, 2015, doi: 10.2815/454889.

[15] N. Tavabi, N. Bartley, A. Abeliuk, S. Soni, E. Ferrara, and K. Lerman, “Characterizing activity on the deep and dark web,” Web Conf. 2019 - Companion World Wide Web Conf. WWW 2019, pp. 206–213, 2019, doi: 10.1145/3308560.3316502.

[16] D. Moore and T. Rid, “Cryptopolitik and the darknet,” Survival (Lond)., vol. 58, no. 1, pp. 7–38, Jan. 2016, doi: 10.1080/00396338.2016.1142085.

[17] N. Malik, “Terror in the Dark,” London, 2018. [Online]. Available: http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf.

[18] S. Alayda, N. A. Almowaysher, F. Alserhani, and M. Humayun, “Terrorism on Dark Web,” vol. 12, no. 10, pp. 3000–3005, 2021.

[19] Statista, “Global economic costs of terrorism 2019,” 2021. https://www.statista.com/statistics/489649/global-economic-costs-of-terrorism/ (accessed May 09, 2021).

[20] U. N. H. C. for H. Rights, “Negative effects of terrorism on the enjoyment of all human rights and fundamental freedoms,” Ge, vol. 23159, no. December 2016, 2016, [Online]. Available:

https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/444/16/PDF/G1644416.pdf?OpenElement.

[21] Statista, "Number of fatalities due to terrorist attacks worldwide between 2006 and 2019," 2021. https://www.statista.com/statistics/202871/number-of-fatalities-by-terrorist-attacks-worldwide/ (accessed May 09, 2021).

[22] H. Bardwell and M. Iqbal, "The Economic Impact of Terrorism from 2000 to 2018," Peace Econ. Peace Sci. Public Policy, 2020, doi: 10.1515/peps-2020-0031.

[23] N. ÇELİK and M. KARAÇUKA, "Terör Saldırılarının Yerli ve Yabancı Turistlerin Destinasyon Tercihleri Üzerindeki Etkileri: Türkiye İBBS-II Bölgeleri'ne Yönelik Mekansal Bir Analiz," Akdeniz Üniversitesi İktisadi ve İdari Bilim. Fakültesi Derg., pp. 204–222, May 2019, doi: 10.25294/auiibfd.559403.

[24] Y. Özkaya and T. Şimşek, "THE RELATIONSHIP BETWEEN TERRORISM AND FINANCIAL STRUCTURE TERÖR VE FİNANSAL YAPI ARASINDAKİ İLİŞKİ ÖZ," 2017.

[25] BBC, "Iraq's Yazidi community buries 104 victims of IS massacre," Feb. 07, 2014. https://www.bbc.com/news/world-middle-east-55968068 (accessed May 28, 2021).

[26] RAND, "Terrorist Organizations," 2021. https://www.rand.org/topics/terrorist-organizations.html (accessed May 09, 2021).

[27] IEP, "GLOBAL TERRORISM INDEX 2020," 2020.

[28] E. C. Viano, "Cybercrime: Definition, Typology, and Criminalization Defining Cybercrime," 2017, doi: 10.1007/978-3-319-44501-4_1.

[29] A. Chandra and M. J. Snowe, "A taxonomy of cybercrime: Theory and design," Int. J. Account. Inf. Syst., vol. 38, Sep. 2020, doi: 10.1016/J.ACCINF.2020.100467.

[30] S. Gordon and R. Ford, "On the definition and classification of cybercrime," J. Comput. Virol., vol. 2, no. 1, pp. 13–20, Aug. 2006, doi: 10.1007/S11416-006-0015-Z.

[31] C. Wu and J. Wang, "Analysis of Cyberterrorism and Online Social Media," vol. 351, no. Mmetss, pp. 925–927, 2019.

[32] G. Weimann, "Terror in Cyberspace," 2009. https://www.researchgate.net/publication/45380139_Terror_in_Cyberspace (accessed May 28, 2021).

[33] G. Weimann, "Going Dark: Terrorism on the Dark Web," Stud. Confl. Terror., vol. 39, no. 3, pp. 195–206, 2016, doi: 10.1080/1057610X.2015.1119546.

[34] CTIT, "Countering the Use of the Internet for Terrorist Purposes— Legal and Technical Aspects," 2011. Accessed: May 09, 2021. [Online]. Available: www.un.org/terrorism/internet.

[35] J. Qin, Y. Zhou, E. Reid, G. Lai, and H. Chen, "Analyzing terror campaigns on the internet: Technical sophistication, content richness, and Web interactivity," Int. J. Hum. Comput. Stud., vol. 65, no. 1, pp. 71–84, Jan. 2007, doi: 10.1016/j.ijhcs.2006.08.012.

[36] K. Hausken, "The dynamics of terrorist organizations," Oper. Res. Perspect., vol. 6, Jan. 2019, doi: 10.1016/j.orp.2019.100120.

[37] D. Harman, "U.S.-based ISIS cell fundraising on the dark web, new evidence suggests - Haaretz Com - Haaretz.com," Apr. 10, 2015. https://www.haaretz.com/.premium-isis-uses-bitcoin-for-fundraising-1.5366305 (accessed Jan. 24, 2021).

[38] The Institute for National Security Studies (INSS), "Backdoor Plots: The Darknet as a Field for Terrorism," 2013. https://www.inss.org.il/index.aspx?id=4538&articleid=5574 (accessed Jan. 24, 2021).

[39] Ş. Pektaş and J. Leman, "Militant Jihadism Today and Tomorrow," 2019.

[40] MEMRI, "The 'Dark Web' And Jihad: A Preliminary Review Of Jihadis' Perspective On The Underside Of The World Wide Web ," May 21, 2014. https://www.memri.org/jttm/dark-web-and-jihad-preliminary-review-jihadis-perspective-underside-world-wide-web (accessed Jan. 28, 2021).

[41] A. Stenersen, Al-Qaida's Quest for Weapons of Mass Destruction: The History behind the Hype. VDM Verlag Dr. Müller, 2008.

[42] G. D. Koblentz, "Emerging Technologies and the Future of CBRN Terrorism," Wash. Q., vol. 43, no. 2, pp. 177–196, Apr. 2020, doi: 10.1080/0163660X.2020.1770969.

[43] BBC, "Munich shooting: Manhunt after deadly attack at shopping centre - BBC News," 2016. https://www.bbc.com/news/world-europe-36870874 (accessed Jan. 22, 2021).

[44] R. Bender and C. Alessi, "Munich Shooter Likely Bought Reactivated Pistol on Dark Net - WSJ," Jul. 24, 2016. https://www.wsj.com/articles/munich-shooter-bought-recommissioned-pistol-on-dark-net-1469366686 (accessed Jan. 22, 2021).

[45] V. Vilic, "DARK WEB, CYBER TERRORISM AND CYBER WARFARE: DARK SIDE OF THE CYBERSPACE," 2007. https://www.researchgate.net/publication/324720749_DARK_WEB_CYBER_TERRORISM_AND_CYBER_WARFARE_DARK_SIDE_OF_THE_CYBERSPACE (accessed May 10, 2021).

[46] Clarivate, "Web of Science," 2021. https://clarivate.com/webofsciencegroup/solutions/web-of-science/ (accessed Sep. 22, 2021).

[47] J. Qin, Y. Zhou, G. Lai, E. Reid, M. Sageman, and H. Chen, "The dark web portal project: Collecting and analyzing the presence of terrorist groups on the web," in Lecture Notes in Computer Science, 2005, vol. 3495, pp. 623–624, doi: 10.1007/11427995_78.

[48] J. Qin, Y. Zhou, E. Reid, G. Lai, and H. Chen, "Unraveling International Terrorist Groups' exploitation of the Web: Technical sophistication, media richness, and web interactivity," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2006, vol. 3917 LNCS, pp. 4–15, doi: 10.1007/11734628_2.

[49] J. Xu, H. Chen, Y. Zhou, and J. Qin, "On the topology of the dark web of terrorist groups," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2006, vol. 3975 LNCS, pp. 367–376, doi: 10.1007/11760146_32.

[50] J. R. Scanlon and M. S. Gerber, "Forecasting Violent Extremist Cyber Recruitment," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 11, pp. 2461–2470, Nov. 2015, doi: 10.1109/TIFS.2015.2464775.

[51] T. Sabbah, A. Selamat, M. H. Selamat, R. Ibrahim, and H. Fujita, "Hybridized term-weighting method for Dark Web classification," Neurocomputing, vol. 173, pp. 1908–1926, 2016, doi: 10.1016/j.neucom.2015.09.063.

[52] S. Celik, "Tertiary-level internet users' opinions and perceptions of cyberhate," Inf. Technol. People, vol. 31, no. 3, pp. 845–868, May 2018, doi: 10.1108/ITP-05-2017-0147.

[53] J. Dalins, C. Wilson, and M. Carman, "Criminal motivation on the dark web: A categorisation model for law enforcement," Digit. Investig., vol. 24, pp. 62–71, Mar. 2018, doi: 10.1016/j.diin.2017.12.003.

[54] J. K. Saini and D. Bansal, "A Comparative Study and Automated Detection of Illegal Weapon Procurement over Dark Web," Cybern. Syst., vol. 50, no. 5, pp. 405–416, Jul. 2019, doi: 10.1080/01969722.2018.1553591.

[55] Y. Yang, A. R. Pah, and B. Uzzi, "Quantifying the future lethality of terror organizations," Proc. Natl. Acad. Sci. U. S. A., vol. 116, no. 43, pp. 21463–21468, Oct. 2019, doi: 10.1073/pnas.1901975116.

[56] A. Alharbi et al., "A Link Analysis Algorithm for Identification of Key Hidden Services," Comput. Mater. Contin., vol. 68, no. 1, pp. 877–886, Mar. 2021, doi: 10.32604/cmc.2021.016887.

[57] R. H. Kallet, "How to Write the Methods Section of a Research Paper," Respir. Care 49, pp. 1229–1232, 2004.

[58] M. Edwards, A. Rashid, and P. Rayson, "A systematic survey of online data mining technology intended for law enforcement," ACM Comput. Surv., vol. 48, no. 1, Sep. 2015, doi: 10.1145/2811403.

[59] G. Kalpakis et al., "OSINT and the dark web," in Advanced Sciences and Technologies for Security Applications, Springer, 2016, pp. 111–132.

[60] D. Jaclin, "Poached lives, traded forms: Engaging with animal trafficking around the globe," Soc. Sci. Inf., vol. 55, no. 3, pp. 400–425, Sep. 2016, doi: 10.1177/0539018416648233.

[61] A. AL-Imam et al., "Captagon: use and trade in the Middle East," Hum. Psychopharmacol., vol. 32, no. 3, May 2017, doi: 10.1002/hup.2548.

[62] K. Paul, "Ancient Artifacts vs. Digital Artifacts: New Tools for Unmasking the Sale of Illicit Antiquities on the Dark Web," Arts, vol. 7, no. 2, p. 12, Mar. 2018, doi: 10.3390/arts7020012.

[63] A. R. Thomas and R. M. Schwartz, "At-risk populations to unintentional and intentional fentanyl and fentanyl+ exposure," J. Transp. Secur., vol. 12, no. 3–4, pp. 73–82, Dec. 2019, doi: 10.1007/s12198-019-00202-1.

[64] H. Chen, W. C. Chung, J. Qin, E. Reid, M. Sageman, and G. Weimann, "Uncovering the DarkWeb: A Case Study of Jihad on the Web," J. Am. Soc. Inf. Sci. Technol., vol. 59, no. 8, pp. 1347–1359, 2008, doi: 10.1002/asi.

[65] H. Chen, "From Terrorism Informatics to Dark Web Research," 2011, pp. 317–341.

[66] A. Baravalle, M. S. Lopez, and S. W. Lee, "Mining the Dark Web: Drugs and Fake Ids," IEEE Int. Conf. Data Min. Work. ICDMW, vol. 0, pp. 350–356, 2016, doi: 10.1109/ICDMW.2016.0056.

[67] CIGI-IPSOS, "2019 CIGI-Ipsos Global Survey on Internet Security and Trust," 2019. https://www.cigionline.org/internet-survey-2019 (accessed Mar. 20, 2021).

[68] A. Silke, "Research on Terrorism," 2008, pp. 27–50.

[69] Y. Yang, A. R. Pah, and B. Uzzi, "Quantifying the future lethality of terror organizations," vol. 116, no. 43, pp. 21463–21468, 2019, doi: 10.1073/pnas.1901975116.

[70] A. Belasco, "The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11," 2014. Accessed: Jun. 02, 2021. [Online]. Available: www.crs.gov.

[71] F. . Stokman, "Social Network Analysis," Int. Encycl. Soc. Behav. Sci., 2001, Accessed: Apr. 27, 2021. [Online]. Available: https://www.sciencedirect.com/topics/social-sciences/social-network-analysis.

[72] S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan, "Evolution of dark web threat analysis and detection: A systematic approach," IEEE Access, vol. 8, pp. 171796–171819, 2020, doi: 10.1109/ACCESS.2020.3024198.

[73] N. Memon and H. L. Larsen, "Investigative Data Mining Toolkit: A Software Prototype for Visualizing, Analyzing and Destabilizing Terrorist Networks," Vis. Netw. Inf., pp. 1–24, 2006.

[74] A. Luo, "What is content analysis and how can you use it in your research?," 2019. https://www.scribbr.com/methodology/content-analysis/ (accessed Jun. 03, 2021).

[75] A. S. Beshiri and A. Susuri, "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review," J. Comput. Commun., vol. 07, no. 03, pp. 30–43, 2019, doi: 10.4236/jcc.2019.73004.

[76] R. Zheng, Y. Qin, Z. Huang, and H. Chen, "Authorship analysis in cybercrime investigation," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 2665, pp. 59–73, 2003, doi: 10.1007/3-540-44853-5_5.

[77] M. Jordan, D. M. Blei, A. Y. Ng, and J. B. Edu, "Latent Dirichlet Allocation Sampling and Bayesian inference View project EM and optimization algorithms in statistical models View project Latent Dirichlet Allocation Michael I. Jordan," 2003. Accessed: Aug. 04, 2020. [Online]. Available: https://www.researchgate.net/publication/221620547.

[78] Y. Zhou, J. Qin, E. Reid, G. Lai, and H. Chen, "Studying the presence of terrorism on the web," 2005, p. 402, doi: 10.1145/1065385.1065505.

[79] H. Chen, "Dark Web Forum Portal," Springer, New York, NY, 2012, pp. 257–270.

[80] A. Panchenko, A. Mitseva, M. Henze, F. Lanze, K. Wehrle, and T. Engel, "Analysis of Fingerprinting Techniques for Tor Hidden Services," 2017, doi: 10.1145/3139550.3139564.

[81] A. A. AlQahtani and E. S. M. El-Alfy, "Anonymous connections based on onion routing: A review and a visualization tool," Procedia Comput. Sci., vol. 52, no. 1, pp. 121–128, 2015, doi: 10.1016/j.procs.2015.05.040.

[82] H. Prunckun, "Scientific Methods of Inquiry for Intelligence Analysis," Rowman & Littlefield, Sep. 05, 2014. https://www.amazon.com.tr/Scientific-Methods-Inquiry-Intelligence-Analysis/dp/1442224320 (accessed Jun. 03, 2021).