



Review article

Darkweb research: Past, present, and future trends and mapping to sustainable development goals

Raghu Raman^{a,*}, Vinith Kumar Nair^a, Prema Nedungadi^b, Indrakshi Ray^c, Krishnashree Achuthan^d

^a Amrita School of Business, Amrita Vishwa Vidyapeetham, Amritapuri, Kerala, India

^b Amrita School of Computing, Amrita Vishwa Vidyapeetham, Amritapuri, Kerala, India

^c Department of Computer Science, Colorado State University, USA

^d Center for Cybersecurity Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri, Kerala, India

ARTICLE INFO

Keywords:

Darknet
Science mapping
Sustainable development goal
Cybercrime
Cryptomarket
ethics
social policy
social behavior
social psychology

ABSTRACT

The Darkweb, part of the deep web, can be accessed only through specialized computer software and used for illegal activities such as cybercrime, drug trafficking, and exploitation. Technological advancements like Tor, bitcoin, and cryptocurrencies allow criminals to carry out these activities anonymously, leading to increased use of the Darkweb. At the same time, computers have become an integral part of our daily lives, shaping our behavior, and influencing how we interact with each other and the world. This work carries out the bibliometric study on the research conducted on Darkweb over the last decade. The findings illustrate that most research on Darkweb can be clustered into four areas based on keyword co-occurrence analysis: (i) network security, malware, and cyber-attacks, (ii) cybercrime, data privacy, and cryptography, (iii) machine learning, social media, and artificial intelligence, and (iv) drug trafficking, cryptomarket. National Science Foundation from the United States is the top funder. Darkweb activities interfere with the Sustainable Development Goals (SDG) laid forth by the United Nations to promote peace and sustainability for current and future generations. SDG 16 (Peace, Justice, and Strong Institutions) has the highest number of publications and citations but has an inverse relationship with Darkweb, as the latter undermines the former. This study highlights the need for further research in bitcoin, blockchain, IoT, NLP, cryptocurrencies, phishing and cybercrime, botnets and malware, digital forensics, and electronic crime countermeasures about the Darkweb. The study further elucidates the multi-dimensional nature of the Darkweb, emphasizing the intricate relationship between technology, psychology, and geopolitics. This comprehensive understanding serves as a cornerstone for evolving effective countermeasures and calls for an interdisciplinary research approach. The study also delves into the psychological motivations driving individuals towards illegal activities on the Darkweb, highlighting the urgency for targeted interventions to promote pro-social online behavior.

* Corresponding author.

E-mail addresses: raghu@amrita.edu (R. Raman), vinithkumarnair@am.amrita.edu (V. Kumar Nair), prema@amrita.edu (P. Nedungadi), Indrakshi.Ray@colostate.edu (I. Ray), krishna@amrita.edu (K. Achuthan).

<https://doi.org/10.1016/j.heliyon.2023.e22269>

Received 6 April 2023; Received in revised form 8 November 2023; Accepted 8 November 2023

Available online 17 November 2023

2405-8440/© 2023 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

1. Introduction

The Darkweb or Darknet is an intrinsic part of the deep web but represents the darker and regressive side of the world wide web. Key characteristics of the Darkweb include the inability to search or list them through legal platforms, passwords to gain entry when accessible, and hidden identities of users, network traffic, IP addresses, and data exchanged through them [1]. While Darkweb was originally built for military communication and advocating freedom of speech, it has also provided technology enablement and power to adversaries to masquerade heinous activities. These range from extortion, exploitation of humans and children, illegal trade of banned substances or weapons, and promotion of terrorism and radicalism, which directly sabotage the security of people, communities, and the environment. Authors identified the prominent roles of the Darkweb as an e-commerce market, a communication platform, an enabler for cybercrimes and untraceable financial transactions, a source of threat intelligence, and a proxy to the web [2]. How could Darkweb enable all this so easily? Two novel technologies, i.e., the Tor network (or Onion routers) and cryptocurrency bitcoin, complemented the anonymity requirements of users and financial exchange without traceability. Studies and developments on the use and misuse of the Darkweb are relatively recent, with publications on these topics beginning around 2010.

While the Darkweb has been mostly known to fuel crime-as-a-service, the diversity of challenges in combating them and evolving cyber threat intelligence simultaneously remain the top objectives of Darkweb research. The complexities in policy regulations around Darkweb are discussed in some studies [3]. Due to the extensive convoluted procedures, enforcing regulations or shutting down the gateways to Darkweb bridges or relays is nearly impossible. That said, most research has been focussed on developing tools and techniques for detecting criminal and terror provocative activities [4] and cyber threat intelligence [1] that draw valuable insights from various sources on the surface web and Darkweb. The exploratory data analysis is a good example of early work in scrawling and analyzing Darkweb marketplaces to answer basic linchpins such as what, when, which, and how aspects of crime enablers [5]. Attempts to develop an automated operational system that aided the detection and alerting of new malware or exploits in the Darkweb through machine learning and artificial intelligence integration with accuracy levels >80% have also been done [6].

Some recent research on uncovering the characteristics of Darkweb sites reveals that law enforcement agencies are constantly challenged in identifying signals of potential threats for attacks or data breaches within the Darkweb. Addressing this issue, researchers [7] have successfully demonstrated the use of LDA (Latent Dirichlet Allocation) and a non-parametric HMM (Hidden Markov Model) to spot anomalous behaviors. Their techniques identified popular discussion topics in the Darkweb and diagnosed a state transition or change in topics bound to happen around any unique event. Going beyond the topics of interest, the need to identify perpetrators directly benefits law enforcement. While authorship identification using Artificial intelligence techniques has been explored in the literature, this has yet to be attempted for Darkweb. These objectives have been addressed by building authorship verification and identification datasets and exposing the challenges of using NLP techniques [8]. With the protective armor of privacy, the accessible conversations fall short in aiding author identification due to the multi-lingual, mixed-style, and covert communication characteristics within the Darkweb.

COVID-19 has caused widespread fear, anxiety, and panic, increasing the use of the darkweb as people seek to access illegal goods and services. With widespread lockdowns, the use of the darkweb has increased as people have more time to engage in criminal activities. Although Darkweb had incited crime, the pandemic significantly exacerbated it. Not only did Darkweb serve as an information resource, but it also promoted apprehension and conspiracy theories. Deterioration in behavioral traits such as loneliness and gambling were more frequent and correlated to the use of the Darkweb [9]. During COVID-19, the illicit trade of vaccines was rampant, along with factitious proof of vaccination [10]. When shortages arose in regular marketplaces of various COVID-19 medications, the Darkweb showed their high availability and vice versa. This poses high public health risks, especially when regulatory bodies can no longer control prices and availability. With the pandemic stalling or halting activities in the physical world, similar repercussions were witnessed in Darknet markets as per some self-reported studies [11,12]. However, some researchers suggest hoarding addictive drugs due to the perception of potential shortage as a trigger to use Darkweb during the pandemic [13].

The United Nations Sustainable Development Goals (SDG) aim to promote peace and sustainability for current and future generations. However, the Darkweb operates in opposition to these objectives. The SDGs were established at the Rio+20 Summit in 2012 as a global call to action to end poverty, protect the planet, and ensure peace and prosperity for all. Then, the SDGs were formally adopted by the United Nations General Assembly in September 2015.

The connection between the Darkweb and the SDG is indirect, as the Darkweb is primarily used for illegal activities such as cybercrime, the sale of illegal goods, and the spread of misinformation. These activities can negatively impact the achievement of many of the SDGs, such as SDG 1 (No Poverty), SDG 2 (Zero Hunger), SDG 3 (Good Health and Well-being), SDG 4 (Quality Education), and SDG 16 (Peace, Justice and Strong Institutions). The sale of illegal goods on the Darkweb can fuel organized crime, contributing to poverty and food insecurity and undermining public health and safety. Additionally, spreading misinformation on the Darkweb can negatively impact education and public health outcomes, fuel conflict, and undermine peace and justice. Therefore, research into the Darkweb and its impact on human behavior is crucial for understanding the challenges and implications of achieving the SDG. Despite the significant growth of Darkweb usage and its potential impact on multiple SDGs, there needs to be a more systematic analysis of its alignment with various SDGs.

Our study identifies four key opportunities to build on previous research. Firstly, the study provides a comprehensive bibliometrics analysis of a corpus of 1068 publications from 2012 to 2022, including the pandemic period, which played a crucial role in the Darkweb's use by both legitimate and illegitimate users. Secondly, this study identifies thematic areas of research based on science mapping analysis. Thirdly, while previous studies have examined related topics such as cryptocurrencies and Darkweb [14–16], our study is the first to examine the direct mapping of Darkweb research to SDGs. Lastly, the study identifies potential future research topics and provides a comprehensive overview highlighting under-explored areas that could inform future research.

The study uses a quantitative approach, and a bibliometric analysis is used to address the following research questions.

- RQ1: What are the trends in Darkweb publications and citations?
- RQ2: Which are the highly productive countries, top funders, and associated countries, most cited source titles in Darkweb research?
- RQ3: What is the effect of collaboration on citations?

Table 1

State of the literature regarding Darkweb research.

Title	Authors	Methodology	Data Source, Publications, Coverage	Key findings
A bibliometric review of cryptocurrencies: how have they grown?	[17]	Bibliometrics analysis	Web of Science - TP:771 Scopus - TP:648 Coverage: 2010–2019	The number of publications has doubled yearly in the last three years, as seen in their study. The review marks the end of the historical part of cryptocurrencies.
A bibliometric review of cryptocurrencies as a financial asset.	[14]	Bibliometric analysis	Web of Science - TP:464 Coverage: 2008–2020	Highlights the importance of such studies in the current trends in online illegal crypto markets, also known as Darknets.
Malware trends on 'Darknet' crypto-markets	[18]	Linguistic analysis of the text string was executed via Python scripting	Data collected- The Onion Route (ToR) Maximum number of products- 8986 Coverage: 2017–2018	Portrayed the short-term trends in malware products and their costs in underground crypto markets
Darkweb and its impact in online anonymity and privacy: A critical analysis and review.	[19]	Relays that run on Tor network	Data collected- The Onion Route (TOR) Coverage: 2018	Darkweb significantly influences society, and anonymity is a key element of this Influence.
Evolution of dark web threat analysis and detection: A systematic approach	[20]	Systematic Literature Review (SLR)	IEEE Xplore, Science Direct, Springer, Scopus, ACM Digital Library and Google Scholar- TP:65 Coverage: 2003–2019	Darkweb forums are crucial for forensic investigations, as anonymity can also be used to identify criminals.
Terrorism in Cyberspace: A Critical Review of Dark Web Studies under the Terrorism Landscape	[21]	Systematic Literature Review (SLR)	Web of Science - TP:20	Minimal studies had been done on Darkweb
Systematic Literature Review (SLR) on social media and the Digital Transformation of Drug Trafficking on Darkweb	[22]	Systematic Literature Review (SLR)	IEEE, ACM, CiteSeer, ScienceDirect, Google Scholar, Web of Science and Scopus- TP:79 Coverage: 2015–2021	Need for more primary research to assess the quality and coverage of focused research on drug trafficking and other Darkweb crime.
Research Hotspot and Trend Analysis of Anonymous Communication Based on Citespace	[23]	Bibliometrics	China Knowledge Network (CNKI)- TP:325 Coverage: 2000–2022	The “dark web” and “privacy protection” have remained strong since around 2017 and 2018
Preliminary Findings of the Trends and Patterns of Darknet-Related Criminals in the Last Decade	[24]	Bibliometrics	Web of Science, Conference Proceedings Citation Index – Social Science & Humanities (CPCI-SSH), Social Sciences Citation Index (SSCI), Science Citation Index Expanded (SCI-EXPANDED), Arts & Humanities Citation Index (A&HCI)- TP:49 Coverage: Till June 2022	Insights into the evolution of Darknet-related crimes
An insight into the deep web; Why it matters for addiction psychiatry?	[25]	Non-participant ethnographic qualitative study	Duckduckgo and Google Coverage: January–April 2016	Systematic guide for addiction professionals on the deep web and online drug marketplaces
Assessing the extent and nature of wildlife trade on the dark web	[26]	Keyword analysis	Individual posts from Darkweb- 9852 items	Negligible level of activity related to the illegal trade of wildlife on the dark web relative to the open and increasing trade on the surface web
Cybercrime threat intelligence: A systematic multi-vocal literature review	[16]	Systematic Literature Review	ACM Digital Library, IEEEExplore, Wiley Inderscience, Scopus and Bibsonomy- TP:374 Coverage: 1990–2018	Identified gaps and challenges in the field, providing a roadmap for future research
SoK: An Evaluation of the Secure End User Experience on the Darknet through Systematic Literature Review	[27]	Systematic Literature Review	Google Scholar, ACM Digital Library, ScienceDirect, SSRN, IEEE Xplore, and Sage pub- TP:200 Coverage: Till August 2021	User motivations and the evolution of Darknet intelligence
A Systematic Review on Using Hacker Forums on the Dark Web for Cyber Threat Intelligence	[28]	Systematic Literature Review & Meta-Analysis	Scopus and EBSCO- TP:69	The proposed threat intelligence solutions have been built upon the analysis of different forms of unstructured data, including text, videos, and images.

- RQ4: What are the various themes of Darkweb research based on cluster analysis?
- RQ5: How well does Darkweb research map to SDGs?

2. Related work

Table 1 lists the state of the literature regarding Darkweb research.

In the last decade, cryptocurrencies have gained significant attention. Researchers [17] carried out a bibliometric analysis of the scientific production of cryptocurrencies, specifically Bitcoin and Ethereum, using Tableau, R, and VOSviewer software to analyze data from the Web of Science and Scopus databases. The number of publications has doubled yearly in the last three years, as seen in their study. Their analysis of the evolution of blockchain technology based on these cryptocurrencies was particularly interesting. Another study of 464 research articles [14] on cryptocurrencies in business and management identified four research streams in the literature: cryptocurrency returns, efficiency, portfolio diversification, and regulation. The authors also allude to the agenda for future research in cryptocurrencies. The central role of virtual currencies highlights the importance of such studies in the current trends in online illegal crypto markets, also known as Darknets. The study of these trends [18] focused on the various digital products available in these dark markets, using data collected from relevant websites accessed through The Onion Router (Tor), which allows anonymous and encrypted communication. The data was collected over several months from one of the largest active crypto markets. Dream Market also portrayed the short-term trends in malware products and their costs in underground crypto markets.

The use of the Darknet has become increasingly popular after the study [19] provided an overview of the Influence of the Darkweb in different spheres of society by discussing the number of daily anonymous users of the Darkweb (using Tor) in Kosovo and worldwide. Results are gathered from Ahmia and Onion City Darkweb's search engines, and anonymity is also discussed. The paper calculates the number of users based on IP addresses and country codes and presents the number of users in anonymous networks on the Darkweb. As mentioned, anonymity through tools such as Tor causes the Darkweb to be a breeding ground for illegal activities such as pornography, weapon trafficking, drug trafficking, and terrorism. In a systematic literature review of 65 relevant articles from leading databases [20], the authors analyzed crimes, consequences, and methods to provide direction for cybersecurity researchers and specialists in identifying and addressing emerging crime threats on the Darkweb. The study found that further research is needed to identify criminals and crypto markets. Darkweb forums are crucial for forensic investigations, as anonymity can also be used to identify criminals. The effort in analyzing and processing digital evidence aids law enforcement personnel in capturing criminals and shutting down illicit sites on the Darkweb. A critical analysis of the literature on Darkweb studies related to terrorism was conducted [21]. Results indicated that minimal studies had been done on this topic. They recommend utilizing advanced artificial intelligence, image processing, natural language processing, and other techniques to detect and, more importantly, predict terrorist incidents on the Darkweb.

A follow-on study [22] provides a list of systematic literature reviews (SLRs) for investigating and detecting criminal activities related to the international drug market on online social networking platforms on the Darkweb. The study highlights the need for more primary research to assess the quality and coverage of focused research on drug trafficking and other Darkweb crime incidents, covering a wide range of issues such as illicit online business, organized criminal events, and potential illegal markets. Another study [23] used the bibliometric method to analyze the trend of anonymous communication research between 2000 and 2022, using the Citespace tool to analyze authors, institutions, and journal collaborations. They highlighted "Darkweb" and "privacy protection" as keywords that could significantly influence future research. The study also found that the number of publications in the field has rapidly increased. While many prior studies have demonstrated the popular use of the Darkweb for illegal services, a systematic literature review and bibliometric analysis of 49 papers in criminology and penology was carried out [24]. Their study provides valuable insights into the evolution of Darknet-related crimes, including prolific authors, contributions from the Global South, and a need for balance in publications between regions. Six recommendations for future research in this field are also provided, including policing interventions.

An intriguing study [25] provides an overview of current knowledge on prodrug activities on the deep web for mental health and addiction professionals. A non-participant ethnographic qualitative study of prodrug websites on the surface web was conducted using search engines such as DuckDuckGo and Google. Four themes and 14 categories were generated and discussed, including information on accessing the deep web, the Darknet online drug trading sites, search engines, and cryptocurrencies. The paper is a systematic guide for addiction professionals on the deep web and online drug marketplaces. Aside from drugs, illegal wildlife trade also happens on the Darkweb, although the extent of such trade is lower than the open trade on the surface web. One such study [26] found one case of illegal trade related to wildlife related to the sale and discussion of a cactus species used for its hallucinogenic properties. The work discusses the ineffectiveness of enforcement against illegal wildlife trade and the need for more efforts.

As seen above, several studies have characterized the growing magnitude of studies on Darkweb-related crimes. Additionally, there is also burgeoning literature on cyber threat intelligence. A study [16] provides an overview of techniques and indicators for detecting online criminal activity through complex machine and deep learning investigations, as well as threat intelligence and engineering activities across multiple analysis levels (surface, deep, and Darknets) to support law enforcement agencies in effectively combating cybercrime and cyber threats. A systematic analysis of state-of-the-art methods was conducted, including a taxonomy of existing techniques, an overview of detectable criminal activities, and an analysis of indicators and risk parameters. Their work also applied a topic modeling analysis to identify and analyze the most relevant threat concepts in the surface and Darkweb. They also identified gaps and challenges in the field, providing a roadmap for future research. It is well known that the community of Darkweb users is keen on keeping their identities, personal information, and locations secret. The underlying motivations to do so can also serve in improving cybercrime strategies. This was precisely done in one of the studies [27] by systematically analyzing 200 academic papers on Darknet

privacy and security to understand both the user motivations and the evolution of Darknet intelligence. A separate systematic study [28], examines the use of cybercriminal or hacker forums on the Darkweb to develop “cyberthreat intelligence” solutions. The findings indicate that different solutions have been built upon analyzing different forms of unstructured data, such as text, videos, and images, and have different objectives, such as identifying key actors, ranking hackers by expertise, identifying malware, and managing organizational information security risks. However, the proposed solutions must still consider the temporality factor or the important forums’ dynamic nature.

3. Methods

To analyze the field of Darkweb, a bibliometric analysis was conducted. Bibliometric studies use quantitative analysis to examine the productivity, Influence, and other facets of the research environment. The PRISMA-P 2015 framework was used to build the dataset for the analysis [29].

3.1. Bibliometric analysis

Bibliometric analysis serves as a method to discern patterns, themes, and shifts within a particular realm of research. It also facilitates the identification of the most prolific institutions, authors, and countries engaged in that research domain. Researchers employ bibliometric analysis to examine subjects and nations in their studies [30–32,33]. One of its notable advantages is its transparency, reliability, and ease of replication. In this process, it is also useful to carry out map visualization to analyze the structures of knowledge networks [34,35].

The Scopus database [36] was used to find published articles on Darkweb. The rationale behind choosing the Scopus database for sourcing bibliographic data in this study primarily rests on its capacity to meet stringent quality standards for indexation. Moreover, Scopus enjoys popularity due to its comprehensive coverage, encompassing a wide spectrum of journals spanning diverse subject areas. It’s worth noting that Scopus stands out as the foremost citation and abstract database and serves as the most widely employed search [30,37,38]. Science mapping (co-citation, co-authorship, keyword co-occurrence, and bibliographic coupling) and performance analysis (analysis of the number of publications, citations, and their impact) are carried out in this work using bibliometric analysis

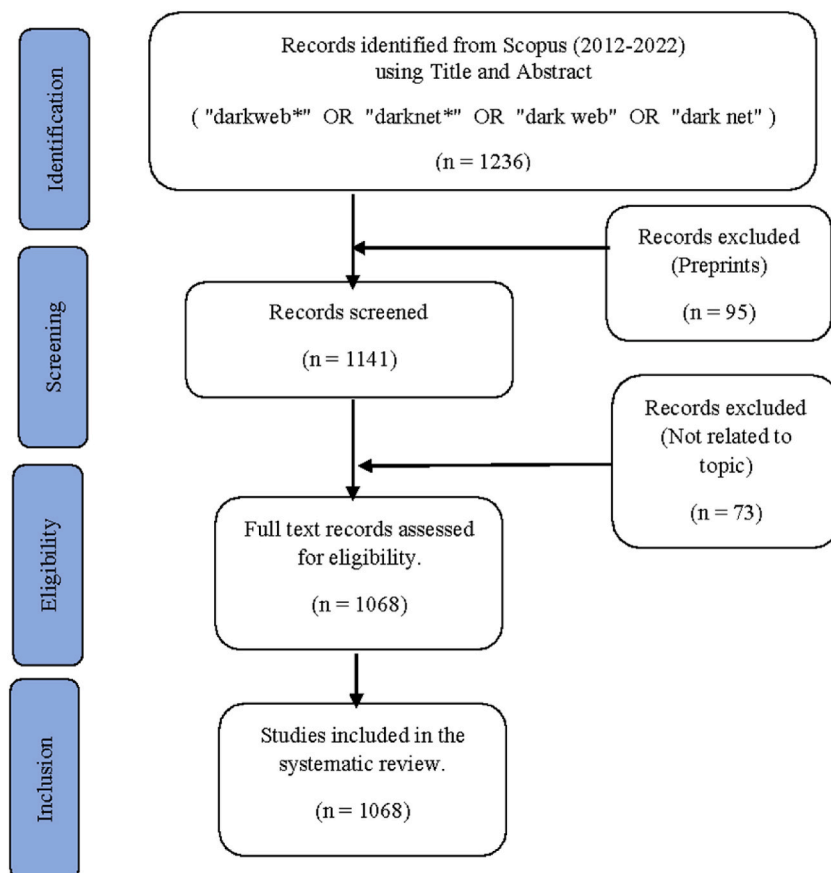


Fig. 1. PRISMA- P 2015 framework.

[35,39]. Topic and countries have been analyzed using bibliometrics [40–42]. In this study, author and index keywords were retrieved and thematically grouped into groups [43] to investigate the evolution of topics published about Darkweb. A quadrant chart has been used to understand the research productivity and Influence [44]. SciVal was used to understand collaborative partnerships and analyze research trends [45]. VOSviewer [46] is used for bibliometric mapping, and keyword clustering [47] has been done as part of the study. Prominence is an indicator of a particular Topic's momentum or visibility. Topic prominence from SciVal was used to arrive at future research directions [48].

3.2. PRISMA protocol

As seen in Fig. 1, five steps as per the PRISMA-P 2015 framework were used to perform a systematic review: establishing a search methodology including databases, search terms, and inclusion/exclusion standards; formulating research objectives; locating relevant material; a title and abstract and full-text screening of the collected literature; and analysis [29]. The PRISMA framework ensures that the selection and analysis of included papers are transparent, offering a reference point for others in the field [24,49].

Using bibliometrics and PRISMA in a single research framework aims to capture a more comprehensive view of the Darkweb research landscape [50]. While PRISMA ensures the inclusion of high-quality, relevant studies through its systematic review guidelines, bibliometrics offers quantifiable metrics on the broader Influence of publications, citations, and thematic clusters within the research domain. Thus, the two methods synergize. This dual approach is particularly beneficial in rapidly evolving or highly interdisciplinary fields like Darkweb, where understanding the intrinsic quality of research and its extrinsic impact is essential.

Publication records ($n = 1236$) were identified from Scopus for the years 2012–2022. We chose 2012 as starting year to coincide with the Rio Summit, where the SDGs were discussed for the first time. Preprints ($n = 95$) and records unrelated to the topic ($n = 73$) were excluded from the search criteria. As part of the screening process, the selected publications were manually checked (abstract, title, keywords, and sometimes conclusions) to ensure they were topically relevant. All the authors were involved in this process. Irrelevant topics were excluded. A total of 1068 records out of 1236 were included in this study. The final dataset was subjected to quantitative bibliometric analyses.

4. Results and discussion

4.1. Research performance

4.1.1. Research productivity (publications) and influence (citations)

Fig. 2 represents the growth of publications in the field of Darkweb over 11 years from 2012 to 2022. Each year, it shows the total publications (TP) and citations (TC). The number of total citations is growing faster than the total publications. In 2012, there were 28 publications with eight citations, while in 2022, there were 169 with 2352 citations. So, the doubling time of publications is 3.67 years, and the Compound Annual Growth Rate (CAGR) is 10%. We observe that post-2015, when SDGs were adopted, publications and citations nearly doubled [51]. The data suggests that the field of Darkweb research has grown and become more established over the past decade, with an increasing number of researchers conducting and citing research on the topic.

4.1.2. Highly productive countries

Using the principles of a quadrant chart, we visualize the research productivity (TP) and Influence (TC) of Darkweb from different countries in four quadrants (Fig. 3).

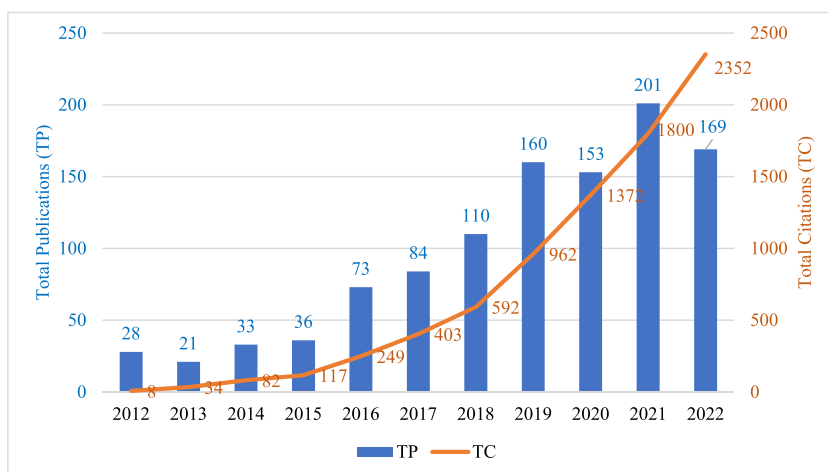


Fig. 2. Research productivity and influence.

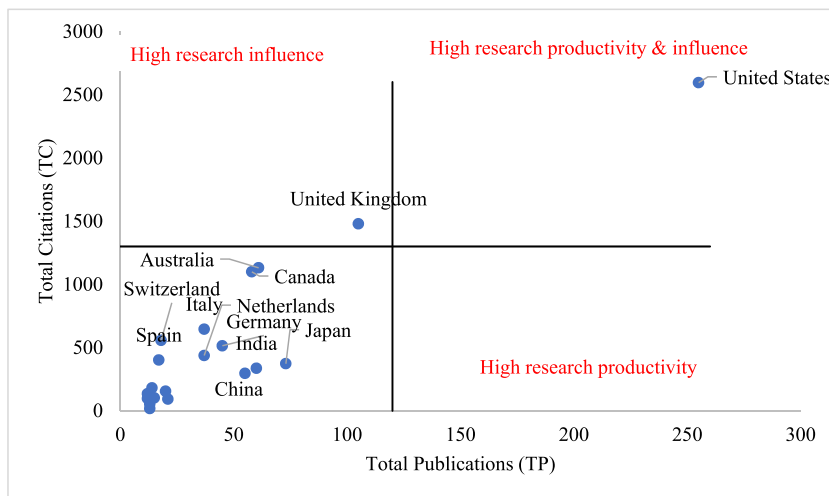


Fig. 3. Highly productive countries.

1. Low research productivity and low research influence: Countries in this quadrant include Japan, Australia, Canada, India, China, Germany, Italy, and the Netherlands.
2. Low research productivity and high research influence: The United Kingdom belongs to this quadrant.
3. High research productivity and low research influence: No countries are in this quadrant.
4. High research productivity and Influence: The United States is the only country in this quadrant.

4.1.3. Top funders and associated countries

Tracking funders helps researchers understand the global distribution of research funding. For example, researchers may be interested in knowing which countries provide the most funding for research in their field or how funding patterns have changed over time [52]. This information can be useful for identifying opportunities for collaboration or for comparing the research funding landscape in different countries. Research on the Darknet will likely interest many countries and organizations due to the potential implications for cybercrime, national security, and internet governance. Governments, law enforcement agencies, and other organizations may, therefore, be interested in funding Darknet research to understand better and address these issues.

According to Table 2, the top three research funders in this list are the National Science Foundation from the United States, the European Commission from Belgium, and the Japan Society for the Promotion of Science from Japan. Six of the top ten funding agencies are from the United States, and one is from China.

4.1.4. Most prolific institutions

Using the principles of a quadrant chart, we can visualize the research productivity (TP) and research influence (TC) of different institutions as follows (Fig. 4).

1. High productivity, high Influence: Examples in this quadrant include the University of New South Wales in Australia, Concordia University in Canada, and Arizona State University in the United States
2. Low productivity, high Influence: The University of Manchester from the United Kingdom and the University of Montreal from Canada belong to this quadrant.

Table 2
Top funders.

Name	Country	TP	TC
National Science Foundation	United States	41	561
European Commission	Belgium	21	391
Japan Society for the Promotion of Science	Japan	14	55
United States Air Force Research Laboratory	United States	10	194
National Natural Science Foundation of China	China	10	69
Directorate for Education & Human Resources	United States	10	75
Directorate for Social, Behavioral & Economic Sciences	United States	10	112
Office of the Director of National Intelligence	United States	9	172
Natural Sciences and Engineering Research Council	Canada	8	120
Office of Naval Research	United States	8	107

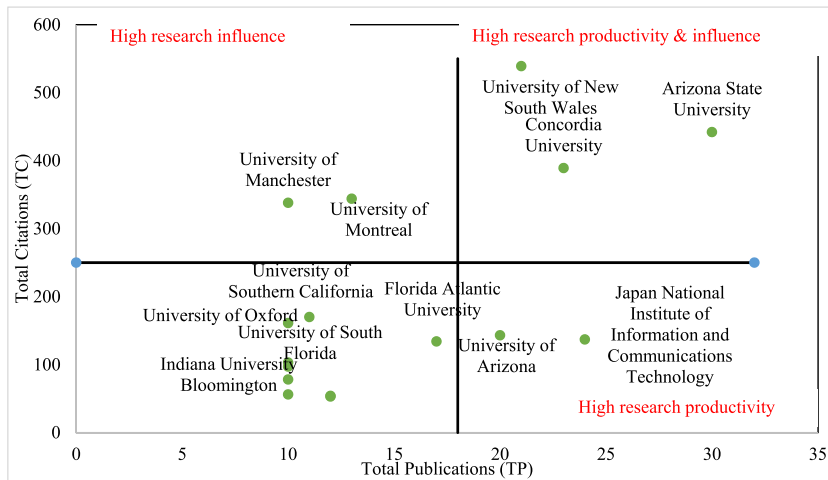


Fig. 4. Most prolific institutions.

- 3. High productivity, low Influence: This quadrant includes the University of Arizona in the United States and the National Institute of Information and Communications Technology in Japan.
- 4. Low productivity, low Influence: This quadrant has the most universities, probably due to their recent focus on Darknet-related research. Examples in this list include Florida Atlantic University in the United States, Technische Universität Darmstadt in Germany, and the University of Oxford in the United Kingdom.

4.1.5. Most cited source titles

According to Table 3, the top three sources for Darkweb research based on the number of publications (TP) are Lecture Notes in Computer Science, ACM International Conference Proceeding Series, and International Journal of Drug Policy. These sources have 50, 36, and 26 papers, respectively. The table also indicates that many other journals and conference proceedings are sources for Darkweb research, including Advances in Intelligent Systems and Computing, Communications in Computer and Information Science, and Studies in Computational Intelligence. Interestingly, conferences and journals are sources for papers in Darkweb research. The table also shows the number of citations (TC) for each source and the TC/TP ratio, which can provide additional information about the impact and significance of the research published in each source.

The top three sources for Darkweb research based on the number of citations (TC) are the International Journal of Drug Policy, Forensic Science International, and Addiction. These sources are all journals and have the highest TC/TP (citations per paper) ratios in the table, with the International Journal of Drug Policy having a TC/TP of 38.3 and Forensic Science International having a TC/TP of 32.3. Green highlighted cells are the highest values in the respective column.

Table 3
Top cited source titles.

Source Title	Source Type	TP	TC	TC/TP
Lecture Notes in Computer Science	Journal	50	158	3.2
ACM International Conference Proceeding Series	Conference	36	117	3.3
International Journal of Drug Policy	Journal	26	995	38.3
Advances in Intelligent Systems and Computing	Journal	13	27	2.1
eCrime Researchers Summit, eCrime	Conference	12	52	4.3
Communications in Computer and Information Science	Conference	12	22	1.8
2018 IEEE International Conference Intelligence & Security Informatics	Conference	8	76	9.5
Forensic Science International	Journal	7	226	32.3
Addiction	Journal	6	166	27.7
Studies in Computational Intelligence	Journal	6	32	5.3

4.1.6. Impact of collaboration

Collaboration can take various forms, such as international collaboration between researchers from different countries, a national collaboration between researchers from the same country, an institutional collaboration between researchers from the same institution. Evidence suggests that international research collaboration can lead to better citations. One study found that international collaboration can increase research visibility and impact and lead to new research networks and partnerships [53]. Another study found that international collaboration was positively correlated with the number of citations received by a research paper [54].

Regarding the impact of collaboration, as seen in Table 4, international collaboration accounts for 20.1% of the total. It has the highest TC/TP ratio of 13.7, while national collaboration accounts for 28.1% of the total and has a TC/TP ratio of 9.2.

4.2. Thematic clusters based on keyword co-occurrence

Fig. 5 shows themes based on keyword co-occurrence. A keyword co-occurrence network focuses on understanding the knowledge components and knowledge structure of a scientific/technical field by examining the links between keywords in the literature. A keyword co-occurrence network is created by treating each keyword as a node and each co-occurrence of a pair of words as a link between those two words [55,56]. The nodes highlight the keywords, and the size of the respective nodes reflects the frequencies of co-occurrence of these keywords. Node size and line thickness are positively related to the keyword connection; the larger the node, the higher the frequency of the keyword, and the thicker the line, the closer the connection between the two topics.

We used VOSviewer [46,47] to create a visualization of the keyword co-occurrence network. Our unit of analysis was “index keywords.” We extracted a total of 5155 index keywords from the dataset, and 55 keywords met the inclusion criterion when the minimum number of keyword occurrences was set to 15. We also carefully used the VOSviewer thesaurus feature to merge synonyms of certain keywords into a single term. All of these criteria were helpful for reducing the number of keywords in the network, the number of clusters, and the complexity of the network while maintaining the quality of the interpretation. After applying these criteria, VOSviewer generated a visualization with four distinct clusters (Fig. 5) and Table 5 shows the top keywords in each cluster.

4.2.1. Cluster 1 (blue): Network security, malware, cyber-attacks

The top keywords in this cluster, themed Network Security, Malware, and Cyber-attacks, are shown in Table 6. This cluster exemplifies the usefulness of probing Darknets in their ability to serve as network telescope and cyber intelligence tools while offering benefits to studying large-scale attacks’ evolution. The human behavior of seeking anonymity and engaging in criminal activities on the Darkweb fuels security threats. Understanding the motivations and attitudes of those who participate in these activities on the Darkweb can inform strategies to prevent and mitigate network security breaches, malware attacks, and cyber-attacks. Highly cited articles in this cluster are shown in Table 6 and analyzed further.

The seminal work by researchers [57] is the first set of studies to dive deeply into the amplification hosts. Distributed Denial of Service (DDoS) attacks based on Network Time Protocol (NTP) amplification rose from obscurity to the dominant large DDoS vector. Five datasets were used to characterize the evolution of these attacks and their impact on global Internet traffic, Darknet scanning activity, active probing, global DDoS attack victims and incidents, and local ISP impact. Authors [58] present a survey on the Darknet, a method for passively observing Internet activity and cyber-attacks. They define and characterize the Darknet, compare it to other monitoring systems, and report on case studies. They also identify research gaps in Darknet technologies and find that Darknet projects are distributed in one-third of the global Internet. The authors find that computer worms and scanning activities are the most common threats investigated through the Darknet, but DDoS amplification and spoofing activities are understudied. While the telescopic view of Darknet activities is useful, a microscopic view of the Tor network’s hidden services was attempted [59]. They developed a new dataset called “Darknet Usage Text Addresses” (DUTA) for studying Darknet active domains and the anonymous expression and illegal activity that occurs on the Deep Web. They built DUTA by sampling the Tor network and manually labeling each address into 26 classes. Using DUTA, they compared two text representation techniques and three supervised classifiers to categorize Tor hidden services. These results are preliminary, and more enhanced datasets will offer better detection services to law enforcement authorities.

4.2.2. Cluster 2 (green): cybercrime, data privacy, cryptography

Based on the keywords in this cluster, as seen in Table 5, the theme of Cluster 2 is Cybercrime, Data Privacy, and Cryptography and is closely connected to the illicit drug trade on the Darknet. Cybercrime tools and techniques, like using encrypted communication channels and anonymous online identities, are commonly employed by drug traffickers to protect their identities and evade detection. Highly cited articles in this cluster are shown in Table 7.

A study [60] examined trust and reputation building on Darknet marketplaces where vendors and customers exchange illicit drugs and other goods using hidden internet services. They qualitatively analyze data from a study on small-scale drug dealing and case

Table 4
Impact of collaboration.

Type of collaboration	% share	TC/TP
International	20.1%	13.7
National	28.1%	9.2
Institutional	35.1%	7.6
Single authorship	16.7%	5.9

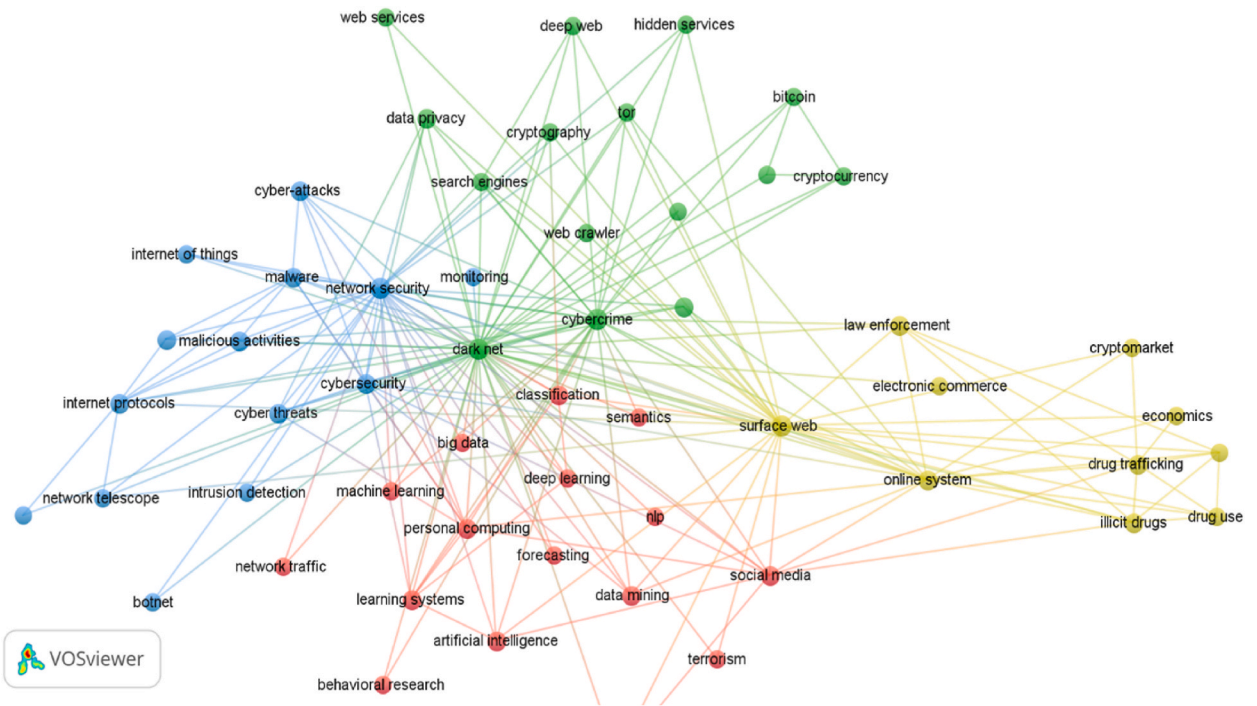


Fig. 5. Thematic clusters based on keyword co-occurrence.

Table 5
Top ten keywords in each cluster with a thematic focus.

Cluster 1 (blue)	Cluster 2 (green)	Cluster 3 (red)	Cluster 4 (yellow)
Network Security, Malware, Cyber-attacks	Cybercrime, Data Privacy, Cryptography	Machine learning, Social media, Artificial intelligence	Drug Trafficking, Cryptomarket
network security	Darknet	machine learning	surface web
cybersecurity	cybercrime	social media	online system
malware	tor	data mining	drug trafficking
internet protocols	data privacy	artificial intelligence	law enforcement
cyber-attacks	criminal activities	classification	cryptomarket
denial-of-service attack	deep web	big data	illicit drugs
malicious activities	search engines	deep learning	drug marketing
cyber threats	bitcoin	web crawler	economics
network telescope	cryptography	terrorism	drug use
botnet	hidden services	nlp	electronic commerce

Table 6
Top cited publications in Cluster 1.

Cluster 1: Network Security, Malware, Cyberattacks	Authors	Year	TC
Taming the 800-pound gorilla: The rise and decline of NTP DDoS attacks	[57]	2014	98
Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization	[58]	2016	71
Classifying illegal activities on tor network based on web textual contents	[59]	2017	54

Table 7

Top cited publications in Cluster 2.

Cluster 2: Cybercrime, Data Privacy, Cryptography	Authors	Year	TC
The transparency paradox. Building trust, resolving disputes and optimizing logistics on conventional and online drugs markets	[60]	2016	76
Learning from the Darkweb: leveraging conversational agents in the era of hyper-privacy to enhance marketing	[61]	2020	60
The Darknet: Self-regulation dynamics of illegal online markets for identities and related services	[62]	2012	41

studies on four online vendors. They find trust is established differently online through anonymizing software, cryptocurrencies, escrow services, and customer feedback systems. They also find differences in violence and logistics practices between online and offline drug markets. Online markets rely on traditional postal services, and offline markets restrict selling to private surroundings to avoid law enforcement. Several Darkweb practices involving technologies are more advanced than those on the surface web, especially regarding privacy-protecting practices while retaining certain aspects of professional surface web services. Researchers [61] hypothesize that over the next 5–10 years, society will become more concerned with privacy on the web, and information-sharing practices currently found on the Darkweb will be adapted to the overall web. Recent developments in the surface web, such as anti-fingerprinting and encrypted communications, already showcase such transitions and adoption. One of the studies [62] investigated the functioning of illegal online markets where identity data, such as data used to access computers, bank accounts, and credit cards, are traded. These markets operate without state regulation and use alternative mechanisms to create participant trust. The paper shows that the sales outlets of these illegal markets can self-regulate and are a significant factor in making cybercrime profitable. Data privacy is also a concern for drug traffickers on the Darknet, as they often need to protect sensitive information such as customer lists and transaction details from being accessed by authorities or rival organizations. Cryptography plays a key role in securing and protecting this sensitive information.

4.2.3. Cluster 3 (red): machine learning, social media, artificial intelligence

Cluster 3 thematic focus is Machine learning, Social media, and Artificial intelligence related to the Darkweb. Machine learning and artificial intelligence techniques can analyze large amounts of social media data to identify patterns and trends related to the illicit drug trade and drug trafficking in the Darkweb. Data mining and classification algorithms can be applied to big data sets to identify suspicious activity and potential threats, making tracking and disrupting illegal drug networks in the Darkweb easier. Highly cited articles in this cluster are shown in Table 8.

The highly cited publication [6] describes an operational system for collecting cyber threat intelligence from various social platforms on the Internet, particularly on the Darknet and deepnet. The system focuses on collecting information from hacker forums and marketplaces. It uses data mining and machine learning techniques to recall 92% of products in marketplaces and 80% of discussions on forums relating to malicious hacking. The system alerts information on newly developed malware and exploits that still need to be deployed in attacks and can be used to assist security experts in threat analysis. While AI and ML can be modeled for the identification and predictability of anomalies, their power to test the extent of anonymity was studied [63] in the context of the Darkweb. Their work investigates the degree to which anonymity tools and the traffic they hide can be identified using machine learning classifiers and a public dataset. The third highest cited publication [64] addresses the limitations of the traditional classification of illicit activities, followed by most AI-based research studies, by proposing a better taxonomy using a two-dimensional model. This significantly enhances the ability to record various crimes more efficiently, allowing automated retrievals.

4.2.4. Cluster 4 (yellow): drug trafficking, cryptomarket

Cluster 4 focuses on drug trafficking and cryptomarket. The Darkweb is a platform for illegal activities such as drug trafficking driven by human behavior, including motivations for seeking illicit substances and financial gain. Psychological factors, such as impulsiveness, lack of self-control, and the need for immediate gratification, can contribute to an individual's involvement in these illegal activities. The anonymous and encrypted nature of the Darkweb allows drug traffickers to operate without fear of detection by law enforcement. Highly cited articles in this cluster are shown in Table 9.

In their study [65], investigated how Darknet market users establish and compare drug quality. They use a two-stage method, analyzing a user forum and conducting qualitative interviews with Darknet users. They find that quality can mean reliability, purity, potency, and predictability of effect and that users draw on embodied, craft, and chemical knowledge to assess quality. The authors conclude that users' evaluations of quality depend on their experience, the purpose of use, and context and that market forums can be useful sources of harm reduction information for users. Cryptomarkets are online marketplaces on the Darkweb that are used to sell illicit drugs. In the second-highest cited publication, authors [66] analyzed data from eight such markets to provide an overview of the Canadian illicit drug market, including the most prevalent drugs for sale, destination countries, and the structure and organization of

Table 8

Top cited publications in Cluster 3.

Cluster 3: Machine learning, Social media, Artificial intelligence	Authors	Year	TC
Darknet and deepnet mining for proactive cybersecurity threat intelligence	[6]	2016	110
Anonymity Services Tor, I2P, JonDonym: Classifying in the Dark (Web)	[63]	2020	49
Criminal motivation on the Darkweb: A categorization model for law enforcement	[64]	2018	28

Table 9
Top cited publications in Cluster 4.

Cluster 4: Drug Trafficking, Cryptomarket	Authors	Year	TC
Concepts of illicit drug quality among Darknet market users: Purity, embodied experience, craft and chemical knowledge	[65]	2016	75
Studying illicit drug trafficking on Darknet markets: Structure and organization from a Canadian perspective	[66]	2016	75
Constructive activism in the Darkweb: cryptomarkets and illicit drugs in the digital ‘demimonde’	[67]	2016	64

distribution networks. The research also looked at how vendors diversify and replicate across marketplaces, the number of listings they manage, and the number of cryptomarkets they are active on. This study shows the importance of online marketplaces in illicit drug trafficking and how analyzing online data can provide knowledge about criminal activities. Aside from the sale of drugs, expression of activism is rampant on Darkweb. The study [67] examines activism on Silk Road, a now defunct cryptomarket on the Darkweb where illicit drugs were sold. The authors conducted anonymous online interviews with people who reported buying drugs on the Silk Road and found that the marketplace facilitated a shared experience of personal freedom within a libertarian framework and allowed for open discussions about stigmatized behaviors.

4.3. Darkweb research mapped to SDG

Research on the Darkweb could provide insights into cybercrime, illicit trade, and other activities that could undermine peace and stability. In our study, we created a co-citation map to uncover the linkages between SDG as measured through citations. The proximity between SDGs indicates how similar they are in co-citation frequency, meaning that publications from two SDGs are often cited together in the same set of publications. The nodes’ size represents the SDG frequency in terms of total publications, and the thickness of the edges represents the frequency of co-citation between SDG. Fig. 6 displays the SDG cluster map for the Darkweb research.

Cluster 1 (red) is dominated by SDG 16, which focuses on peace, justice, and strong institutions. This cluster also has strong connections to other SDGs, including SDG 8 (decent work and economic growth), SDG 9 (industry, innovation, and infrastructure), and SDG 5 (gender equality). Cluster 2 (green) brings together SDG 10 (reduced inequalities), 12 (responsible consumption and production), 13 (climate action), 14 (life below water), and 15 (life on land). This cluster represents a range of environmental and social goals to promote sustainability and reduce negative impacts on the planet.

Table 10 shows a mapping of Darkweb research mapped to SDG based on publications. SDG 16 (Peace, Justice, and Strong Institutions) has the highest number of publications and citations, accounting for 70% of the total publications mapped to SDG. This is followed by SDG 3 (Good Health and Well-Being) at 19%. The SDG with the highest ratio of citations to publications (TC/TP:20.8) is SDG 9 (Industry, Innovation, and Infrastructure).

The Darkweb and SDG 16 have an inverse relationship, as the former undermines the latter. The Darkweb is often used for illegal activities such as human trafficking, drug trafficking, and arms trafficking, which directly contradicts the goal of SDG 16 to promote peaceful and inclusive societies. The illegal activities facilitated by the Darkweb can lead to increased organized crime, money laundering, and corruption, eroding the rule of law and good governance. This can make it difficult for individuals and communities to access justice and can also contribute to instability and violence in societies. The Darkweb can also provide support to organized crime

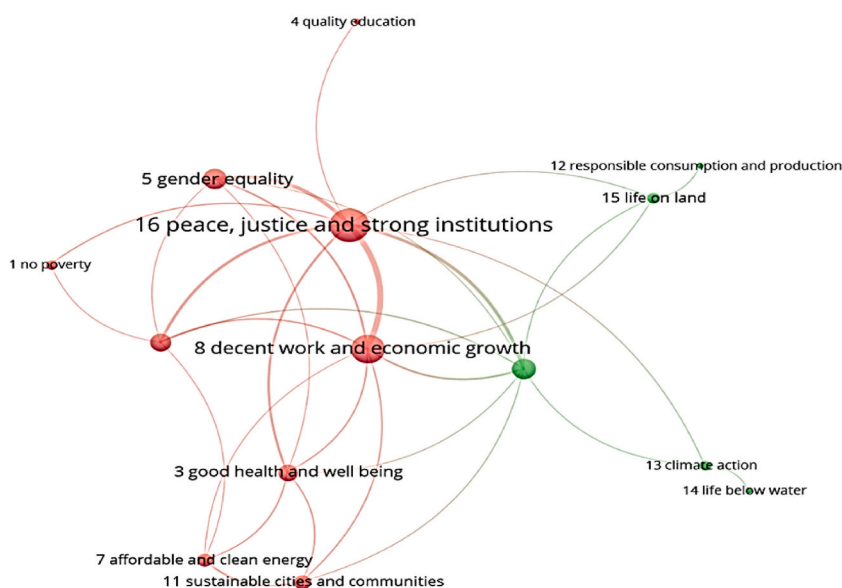
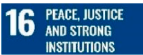






Fig. 6. Co-citation map showing linkages of SDG.

Table 10
Top SDG mapped by Darkweb research publications.

SDG	TP	TC	TC/TP
 16 PEACE, JUSTICE AND STRONG INSTITUTIONS	219	1943	8.9
 3 GOOD HEALTH AND WELL-BEING	59	763	12.9
 8 DECENT WORK AND ECONOMIC GROWTH	9	36	4.0
 9 INDUSTRY, INNOVATION AND INFRASTRUCTURE	8	166	20.8
 4 QUALITY EDUCATION	5	12	2.4

groups that are involved in illegal activities.

The relationship between the Darkweb and SDG 3, which aims to ensure healthy lives and promote well-being for all, can also be described as inverse. The Darkweb is often used as a platform for the illegal drug trade, which can negatively impact public health, such as increasing the availability of harmful substances, substance abuse, and overdose. The Darkweb can also be used to sell counterfeit medicines, which can be dangerous and ineffective and contribute to the spread of disease. It can also be used as a platform to promote online health scams, misleading people into buying fake or ineffective treatments and discouraging people from seeking legitimate medical care. The Darkweb can also be a breeding ground for misinformation, which can negatively impact public health.

The Darkweb can be a barrier to achieving SDG 9 by facilitating the illegal trade of goods and services, such as counterfeit products, stolen intellectual property, and illegal weapons, which can undermine the legitimate economy and discourage investment in legitimate infrastructure and innovation.

According to [Table 11](#), the number of publications related to SDG 16 has increased by over 300% in the last decade, with a particularly steep increase in the last few years. This is a possible healthy sign that researchers are more aware of SDG. For SDG 3, the number of publications increased only after 2015, when SDGs were formally adopted. The total number of publications for the ten years is 59, and the overall growth rate is 633%.

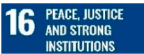

5. Conclusions

The Darkweb, a hidden part of the Internet, attracts individuals who seek to engage in illegal activities while maintaining anonymity. This behavior can be linked to psychological factors such as impulsiveness, thrill-seeking, and a sense of power. The past decade has seen increased publications and citations related to Darkweb research. The United States appears to be the only country with high research productivity and Influence regarding Darkweb. The United Kingdom has low productivity but high Influence, while Japan, Australia, Canada, India, China, Germany, Italy, and the Netherlands fall into low productivity and Influence. Research funding in Darkweb research will likely interest various countries and organizations due to the potential impacts on issues such as cybercrime, national security, and internet governance. The top three funders identified in the data are the National Science Foundation from the United States, the European Commission from Belgium, and the Japan Society for the Promotion of Science from Japan. Six of the top ten funders are from the United States, with one from China. University of New South Wales in Australia, Concordia University in Canada, and Arizona State University in the United States have high research productivity and Influence.

The top three sources for Darkweb research based on the number of publications are Lecture Notes in Computer Science, ACM International Conference Proceeding Series, and the International Journal of Drug Policy. The top three sources based on the number of citations are the International Journal of Drug Policy, Forensic Science International, and Addiction. These sources are all journals and have the highest citations per publication ratio.

Research on the Darkweb, a secretive and often illicit part of the Internet, seems relevant to the UN SDG, particularly SDG 16 (Peace, Justice, and Strong Institutions). According to this study, SDG 16 has the highest number of publications and citations related

Table 11
Evolution of top two SDG.

SDG	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	TP	% Growth
 16 PEACE, JUSTICE AND STRONG INSTITUTIONS	4	4	3	5	17	17	28	33	39	69	219	306%
 3 GOOD HEALTH AND WELL-BEING	0	0	0	0	3	6	9	7	12	22	59	633%

to the Darkweb, followed by SDG 3 (Good Health and Well-Being). There are strong linkages between peace and inequalities (SDG 16 and 10) and peace and good health (SDG 16 and 3), highlighting the centrality of SDG 16.

Four major themes have arisen from the analysis of keyword co-occurrences: Network Security, Malware, and Cyber-attacks; Cybercrime, Data Privacy, and Cryptography; Machine learning, Social media, and Artificial intelligence; and Drug Trafficking and Cryptomarkets. There has been some speculation that the Darknet may have spread misinformation about the COVID-19 pandemic. For example, some have suggested that the Darknet may have been used to spread conspiracy theories or false information about the origins or treatment of the virus [68]. Yet another study published in the journal Health Security found that the Darkweb was being used to sell unproven and potentially dangerous treatments for COVID-19, such as hydroxychloroquine [69].

Understanding the psychological motivations behind individuals' engagement in illegal activities on the Darkweb is crucial in developing effective countermeasures and promoting pro-social behavior online. The psychological impacts on individuals who use the Darkweb for illegal activities, such as anxiety and stress, should also be considered. Incorporating human behavior and psychology elements into Darkweb research can provide a more comprehensive understanding of the phenomenon and inform more effective solutions. Researching the Darkweb can raise ethical considerations, particularly if it involves studying illegal activities or vulnerable populations. Researchers should carefully consider the potential implications of their research and take steps to minimize any potential harm or negative consequences.

The conclusions drawn from this study underscore the multi-dimensional nature of the Darkweb, revealing a complex interplay between technology, psychology, and geopolitical factors. Regarding future research directions, an interdisciplinary approach is indispensable. Combining technological methods, such as advancements in network security and natural language processing, with insights from psychology and geopolitics could yield more comprehensive and effective countermeasures against the challenges posed by the Darkweb.

5.1. Future research directions

Our study identified five potential research directions for Darkweb researchers by ranking the topics based on prominence percentile (Table 12). The prominence of a topic, which reflects its momentum, is calculated using three metrics: the number of citations, the number of views, and the journal Citation score. Typically, Topics with a high prominence percentile will have low publications but will likely be research frontiers. Publications are organized into topics by clustering their citation network. Each topic consists of publications with a common theme and is grouped using a direct citation analysis of the reference lists in the publications. A publication can only belong to one topic.

5.1.1. Darkweb and bitcoin, blockchain, Internet of Things

Bitcoin, blockchain, and the Internet of Things (IoT) are all technologies used in the Darkweb in various ways. For example, the Monero cryptocurrency, which uses a privacy-focused blockchain, has been popular on the Darkweb due to its greater anonymity than other cryptocurrencies like Bitcoin [70]. A blockchain explorer is a tool that allows users to view and analyze the transactions that have taken place on a particular blockchain [71]. It can track funds' movement and identify patterns or anomalies indicating illicit activity. Using private blockchains in agriculture is an interesting application of the technology [72]. A private blockchain can create a secure and transparent record of transactions within a closed network, such as a network of farms or agricultural supply chain partners.

Potential research questions in this area include investigating how the Darkweb is being fuelled by the trade of cryptocurrencies and its implications for legal and regulatory frameworks, studying the usage of blockchain technologies on the Darkweb and its impact on security and privacy, analyzing the relationship between the Darkweb and the IoT and their utilization in facilitating cybercrime and other illicit activities, understanding the strategies employed by law enforcement agencies and other authorities to disrupt and dismantle these networks and the ethical and social implications of the use of these technologies in illegal activities.

5.1.2. Darkweb and embedding, Named entity recognition, entailment

Another research direction being pursued is embedding, named entity recognition, and entailment, all concepts related to natural language processing (NLP), the field of artificial intelligence that deals with the interaction between computers and human (natural) language. NLP techniques can analyze text-based content on the Darknet, such as online forum discussions or listings on Darknet marketplaces. [DarkJargon.net](https://darkjargon.net) is an example of a platform that aims to understand underground conversation on the Darknet by using latent meaning analysis [73]. The platform aims to identify trends and patterns in how individuals communicate about illegal activities by analyzing the language used in online discussions. Named entity recognition in cyber threat intelligence using transformer-based

Table 12
Top topics based on prominence percentile.

Topic	Prominence Percentile
Bitcoin, Blockchain, and the Internet of Things	99.981
Embedding; Named Entity Recognition; Entailment	99.946
Exchange Rates; Cryptocurrency	99.721
Phishing; Cybercrime	98.816
Botnet; Malware	97.689
Digital Forensic; Electronic Crime Countermeasures	97.328

models is another example that can be used to extract structured information from unstructured text and can be applied to analyzing text-based content on the Darknet [74]. DreamDrug is a crowdsourced named entity recognition (NER) dataset for detecting drugs in Darknet markets [75]. By training machine learning models on this dataset, researchers can develop tools for automatically identifying and classifying drugs in online listings on Darknet marketplaces.

Research on this topic could focus on various questions, such as exploring how NLP can be used to analyze the content of the Darkweb and extract information about illegal activities and the networks of individuals and organizations involved in them; utilizing the results of NLP to build predictive models that can help law enforcement agencies to identify and disrupt illegal activities on the Darkweb; Understanding and adherence to the policy regulations for data gathering and processing across multiple countries and identifying and addressing the root causes of illegal activities on the Darkweb, such as social and economic inequalities.

5.1.3. Darkweb and exchange rates, cryptocurrency

Exchange rates and cryptocurrency are both relevant to the Darkweb in many ways. Cryptocurrencies, such as Bitcoin, can be used as a means of payment on the Darkweb, and the value of these cryptocurrencies can fluctuate significantly. This volatility can be a factor in their use of the Darkweb. The use of cryptocurrencies in the Darkweb has been the subject of recent studies. These studies have examined the facilitative factors that enable Bitcoin-related crimes on the Darkweb, such as the anonymity of cryptocurrencies and the lack of regulation in certain jurisdictions [76]. Other studies have explored the ethical implications of using cryptocurrencies for illegal purposes and the potential for regulation to address this issue [77]. Research on currency substitution in the shadow economy, which includes the Darkweb, has also examined the use of Bitcoin and other cryptocurrencies as an alternative to traditional fiat currencies [78]. This research has used local Bitcoin trade volume as a proxy for adopting cryptocurrencies in the shadow economy and has found evidence of currency substitution in some cases.

Future research in the field of cryptocurrency in the Darkweb could focus on various questions, such as studying the impact of exchange rates and other economic factors on the use of cryptocurrency in the Darkweb and its implications for the stability and security of these currencies and analyzing the trends in the use of different cryptocurrencies on the Darkweb and comparing them to their usage in other contexts.

5.1.4. Darkweb and phishing, cybercrime

The Darkweb is often associated with cybercrime, including phishing attacks. Recent studies have detected phishing and other malicious activity in the Darkweb [79]. For example, developing machine learning techniques and data analytics tools can help identify and track phishing campaigns and other forms of cybercrime [80]. Another research has focused on using active probing-based schemes and data analytics to investigate malicious fast-flux web-cloaking-based domains, often used in phishing attacks [81]. These schemes involve automated tools to probe suspected domains and gather information about their activity and characteristics.

Several potential research areas are related to the Darkweb, phishing, and cybercrime. These could include investigating the motivations, persona, and behavior of cybercriminals operating in the Darkweb, developing techniques for tracking and disrupting cybercrime activity in the Darkweb, finding ways to prevent individuals from falling victim to phishing attacks, and researching the ways organizations respond to cyber-attacks and developing methods to improve the effectiveness of responses to mitigate the effects of cyber-attacks.

5.1.5. Darkweb and botnet, malware

The Darkweb is often used as a platform for distributing botnets and malware, which are tools that can be used for various malicious purposes, including distributed denial of service (DDoS) attacks, spamming, and identity theft. One example of recent research in this area is the analysis of a '0' stealth scan from a botnet [82]. This study examined the characteristics and behavior of a particular type of botnet and attempted to identify the motivations and tactics of the attackers behind it. Other research has focused on identifying the most influential suspicious domains in the Tor network, a network of servers that can be used to access the Darkweb [83]. This research used a machine learning technique called "ToRank" to identify and rank the most influential domains based on their activity and connections to other domains [84]. There has also been research on the detection of botnet activities through the lens of a large-scale Darknet, which involves the analysis of large amounts of data from the Darkweb to identify patterns and trends in botnet activity. Finally, there has been research on using Darkweb crawlers to uncover suspicious and malicious websites on the Darkweb [85].

Research in this area could focus on questions such as developing methods to track and disrupt botnet activity in the Darkweb, understanding the motivations and behavior of cybercriminals who use botnets for attacks, identifying and mitigating the effects of malware attacks, and protecting against the proliferation of malware on the Darkweb by studying how malware is distributed on the Darkweb, developing strategies to disrupt these distribution networks and developing new techniques for identifying and tracking botnet command-and-control servers.

5.2. Theoretical, practical, and policy implications

5.2.1. Theoretical implications

- The findings of this study have important theoretical implications for understanding the Darkweb, its users, and its potential impacts on society. First, the study highlights the multi-dimensional nature of the Darkweb, which is influenced by a complex interplay between technological, psychological, and geopolitical factors. This understanding is essential for developing effective countermeasures to the challenges posed by the Darkweb.

- Second, the study sheds light on the psychological motivations of individuals who engage in illegal activities on the Darkweb. These motivations are complex and varied, but they can include impulsiveness, thrill-seeking, and a sense of power. Understanding these motivations is crucial in developing effective countermeasures and promoting pro-social behavior online.
- Third, the study highlights the importance of an interdisciplinary approach to Darkweb research. Combining technological methods with insights from psychology and geopolitics can yield more comprehensive and effective countermeasures against the Darkweb.

5.2.2. Practical implications

- The findings of this study also have important practical implications for policymakers and law enforcement agencies. First, the study underscores the need to invest in research and development of new technologies to combat cybercrime and protect national security. This includes developing more effective tools for detecting and disrupting Darkweb-based criminal activity.
- Second, the study highlights the importance of international cooperation in combating Darkweb-related crime. The Darkweb is a global phenomenon, and no single country can effectively address it alone. International cooperation is essential for sharing information, developing joint strategies, and coordinating law enforcement efforts.
- Third, the study underscores the need to educate the public about the Darkweb and its potential dangers. This includes raising awareness of the risks of engaging in illegal activities on the Darkweb, as well as the psychological impacts of such behavior.

5.2.3. Policy recommendations

- Increase investment in research and development of new technologies to combat cybercrime and protect national security. Explore the potential of using machine learning and artificial intelligence to detect and disrupt Darkweb-based criminal activity. These technologies have the potential to revolutionize the way law enforcement agencies combat cybercrime.
- Promote international cooperation in combating Darkweb-related crime. This includes sharing information, developing joint strategies, and coordinating law enforcement efforts.
- Educate the public about the Darkweb and its potential dangers. This includes raising awareness of the risks of engaging in illegal activities on the Darkweb, as well as the psychological impacts of such behavior.
- Develop a better understanding of the psychological motivations of individuals who engage in illegal activities on the Darkweb. This knowledge can be used to develop more effective countermeasures and promote pro-social behavior online.
- The study's linkage to UN SDGs, particularly SDG 16, has policy implications for peace and justice. Policy directives could integrate goals to combat cybercrime and data privacy issues under the umbrella of SDG 16, ensuring coherence with global objectives.
- The identification of top funders could inform policy decisions related to the allocation of resources for research, focusing particularly on issues such as cybercrime and national security.

By implementing these recommendations, policymakers and law enforcement agencies can take steps to mitigate the challenges posed by the Darkweb and protect the public from its potential harm.

5.3. Limitations

Bibliometrics, or statistical analysis to measure the impact and importance of scholarly research, has several limitations. First, bibliometrics can be influenced by factors such as the prestige of the journals in which research is published, the language in which it is written, and the number of authors on a paper [86]. This can lead to a biased view of the impact of certain research. Second, bibliometrics often focuses on measures such as the number of citations a paper receives, which may not accurately reflect the quality or impact of the research [87]. Third, self-citation can affect bibliometrics, where authors cite their work to boost their metrics [88]. This can lead to inflated metrics for certain researchers or institutions. Fourth, bibliometrics needs to consider the context in which research is conducted or how it is used or applied [89]. This can limit the usefulness of bibliometric measures in understanding the true impact of research. Finally, the results of a bibliometric analysis can be influenced by the search terms used. The search terms should be narrow enough for the resulting data to reflect the research on a particular topic accurately. A further limitation of bibliometric analyses that rely on abstract databases such as Scopus or Google Scholar is that the coverage of these databases may need to be completed. These databases may include only some relevant papers, particularly those published in less well-known or less prestigious journals or languages other than English [86]. This can lead to a biased view of the research landscape, as papers not included in the database will not be included in the analysis.

Data availability statement

Data will be made available on reasonable request. Data associated with our study has not been deposited into a publicly available repository.

CRedit authorship contribution statement

Raghu Rama: Writing – review & editing, Writing – original draft. **Vinith Kumar Nair:** Writing – review & editing, Visualization,

Software, Data curation. **Prema Nedungadi**: Writing – review & editing, Writing – original draft, Methodology. **Indrakshi Ray**: Writing – review & editing, Writing – original draft, Data curation. **Krishnashree Achuthan**: Writing – review & editing, Writing – original draft, Methodology, Investigation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

We want to express our immense gratitude to our beloved Chancellor, Mata Amritanandamayi Devi (AMMA), for providing the motivation and inspiration for this research work.

This research received no specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

- [1] R. Basheer, B. Alkhatib, Threats from the dark: a review over darkweb investigation research for cyber threat intelligence, *Journal of Computer Networks and Communications* (2021).
- [2] A. Gupta, S.B. Maynard, A. Ahmad, The Darkweb Phenomenon: A Review and Research Agenda, 2021 arXiv preprint arXiv:2104.07138.
- [3] M. Chertoff, A public policy perspective of the Darkweb, *Journal of Cyber Policy* 2 (1) (2017) 26–38.
- [4] H. Chen, W. Chung, J. Qin, E. Reid, M. Sageman, G. Weimann, Uncovering the Darkweb: a case study of Jihad on the web, *J. Am. Soc. Inf. Sci. Technol.* 59 (8) (2008) 1347–1359.
- [5] M. Bernaschi, A. Celestini, S. Guarino, F. Lombardi, Exploring and analyzing the tor hidden services graph, *ACM Trans. Web* 11 (4) (2017) 1–26.
- [6] E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, P. Shakarian, Darknet and deepnet mining for proactive cybersecurity threat intelligence, in: 2016 IEEE Conference on Intelligence and Security Informatics (ISI), IEEE, 2016, pp. 7–12.
- [7] N. Tavabi, N. Bartley, A. Abeliuk, S. Soni, E. Ferrara, K. Lerman, Characterizing activity on the deep and Darkweb, in: Companion Proceedings of the 2019 World Wide Web Conference, 2019, May, pp. 206–213.
- [8] A. Manolache, F. Brad, A. Barbalau, R.T. Ionescu, M. Popescu, VeriDark: A Large-Scale Benchmark for Authorship Verification on the Darkweb, 2022 arXiv preprint arXiv:2207.03477.
- [9] A. Sirola, J. Nuckols, J. Nyrhinen, T.A. Wilska, The Use of the Darkweb as a COVID-19 Information Source: A Three-Country Study, *Technology in Society*, 2022, 102012.
- [10] A. Bracci, M. Nadini, M. Aliapoulos, D. McCoy, I. Gray, A. Teytelboym, A. Gallo, A. Baronchelli, Vaccines and more: the response of Darkweb marketplaces to the ongoing COVID-19 pandemic, *PLoS One* 17 (11) (2022), e0275288.
- [11] A. Bergeron, D. Décarry-Héty, L. Giommoni, Preliminary findings of the impact of COVID-19 on drugs crypto markets, *Int. J. Drug Pol.* 83 (2020), 102870.
- [12] A. Bergeron, D. Décarry-Héty, L. Giommoni, M.P. Villeneuve-Dubuc, The success rate of online illicit drug transactions during a global pandemic, *Int. J. Drug Pol.* 99 (2022), 103452.
- [13] T. Groshkova, T. Stoian, A. Cunningham, P. Griffiths, N. Singleton, R. Sedefov, Will the current COVID-19 pandemic impact on long-term cannabis buying practices? *J. Addiction Med.* (2020).
- [14] R.N.U.D. Jalal, I. Alon, A. Paltrinieri, A Bibliometric Review of Cryptocurrencies as a Financial Asset, *Technology Analysis & Strategic Management*, 2021, pp. 1–16.
- [15] S. Rai, K. Singh, A.K. Varma, A bibliometric analysis of deep web research during 1997-2019, *DESIDOC Journal of Library & Information Technology* 40 (2) (2020).
- [16] G. Cascavilla, D.A. Tamburri, W.J. Van Den Heuvel, Cybercrime threat intelligence: a systematic multi-vocal literature review, *Comput. Secur.* 105 (2021), 102258.
- [17] F.J. García-Corral, J.A. Cordero-García, J. de Pablo-Valenciano, J. Uribe-Toril, A bibliometric review of cryptocurrencies: how have they grown? *Financial Innovation* 8 (1) (2022) 1–31.
- [18] R. Broadhurst, D. Lord, D. Maxim, H. Woodford-Smith, C. Johnston, H.W. Chung, B. Sabol, Malware Trends on 'Darknet' crypto-Markets: Research Review, Available at: SSRN 3226758, 2018.
- [19] A.S. Beshiri, A. Susuri, Darkweb and its impact in online anonymity and privacy: a critical analysis and review, *J. Comput. Commun.* 7 (3) (2019) 30.
- [20] S. Nazah, S. Huda, J. Abawajy, M.M. Hassan, Evolution of Darkweb threat analysis and detection: a systematic approach, *IEEE Access* 8 (2020) 171796–171819.
- [21] E.D.A. Sönmez, K. Seçkin Codal, Terrorism in Cyberspace: A Critical Review of Darkweb Studies under the Terrorism Landscape, 5, *Sakarya University Journal of Computer and Information Sciences*, 2022.
- [22] R. Rawat, V. Mahor, M. Chouhan, K. Pachlasiya, S. Telang, B. Garg, Systematic literature review (SLR) on social media and the digital transformation of drug trafficking on darkweb, in: *International Conference on Network Security and Blockchain Technology*, Springer, Singapore, 2022, pp. 181–205.
- [23] Y. She, D. Xu, Z. Tan, J. Zhao, Research hotspot and trend analysis of anonymous communication based on Citespace, in: 2022 3rd International Conference on Information Science, Parallel and Distributed Systems (ISPDS), IEEE, 2022, pp. 58–62.
- [24] H.T. Luong, Preliminary findings of the trends and patterns of darknet-related criminals in the last decade, *Secur. J.* (2023).
- [25] L. Orsolini, D. Papanti, J. Corkery, F. Schifano, An insight into the deep web; why it matters for addiction psychiatry? *Hum. Psychopharmacol. Clin. Exp.* 32 (3) (2017), e2573.
- [26] J.R. Harrison, D.L. Roberts, J. Hernandez-Castro, Assessing the extent and nature of wildlife trade on the Darkweb, *Conserv. Biol.* 30 (4) (2016) 900–904.
- [27] F. Tazi, S. Shrestha, J. De La Cruz, S. Das, SoK: an evaluation of the secure end user experience on the Darknet through systematic literature review, *Journal of Cybersecurity and Privacy* 2 (2) (2022) 329–357.
- [28] A. Albizri, A. Nehme, A. Harfouche, A Systematic Review on Using Hacker Forums on the Darkweb for Cyber Threat Intelligence, 2022.
- [29] D. Moher, L. Shamseer, M. Clarke, D. Ghersi, A. Liberati, M. Petticrew, L.A. Stewart, Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement, *Syst. Rev.* 4 (1) (2015) 1–9.
- [30] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, W.M. Lim, How to conduct a bibliometric analysis: an overview and guidelines, *J. Bus. Res.* 133 (2021) 285–296.
- [31] M.A. Khan, D. Pattnaik, R. Ashraf, I. Ali, S. Kumar, N. Donthu, Value of special issues in the journal of business research: a bibliometric analysis, *J. Bus. Res.* 125 (2021) 295–313, <https://doi.org/10.1016/j.jbusres.2020.12.015>.
- [32] S. Verma, A. Gustafsson, Investigating the emerging COVID-19 research trends in the field of business and management: a bibliometric analysis approach, *J. Bus. Res.* 118 (2020) 253–261, <https://doi.org/10.1016/j.jbusres.2020.06.057>.
- [33] R. Raman, K. Achuthan, V.K. Nair, P. Nedungadi, Virtual Laboratories-A historical review and bibliometric analysis of the past three decades, *Educ. Inf. Technol.* 27 (8) (2022) 11055–11087.

- [34] C. Cuccurullo, M. Aria, F. Sarto, Foundations and trends in performance management. A twenty-five years bibliometric analysis in business and public administration domains, *Scientometrics* 108 (2016) 595–611.
- [35] M. Aria, C. Cuccurullo, bibliometrix: an R-tool for comprehensive science mapping analysis, *Journal of informetrics* 11 (4) (2017) 959–975.
- [36] P. Mongeon, A. Paul-Hus, The journal coverage of Web of Science and Scopus: a comparative analysis, *Scientometrics* 106 (2016) 213–228.
- [37] V.N. Amrutha, S.N. Geetha, A systematic review on green human resource management: implications for social sustainability, *J. Clean. Prod.* 247 (2020), 119131.
- [38] J. Paul, W.M. Lim, A. O’Cass, A.W. Hao, S. Bresciani, Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR), *Int. J. Consum. Stud.* 45 (4) (2021) O1–O16.
- [39] M. Gutiérrez-Salcedo, M.Á. Martínez, J.A. Moral-Munoz, E. Herrera-Viedma, M.J. Cobo, Some bibliometric procedures for analyzing and evaluating research fields, *Appl. Intell.* 48 (2018) 1275–1287.
- [40] C. Huang, C. Yang, S. Wang, W. Wu, J. Su, C. Liang, Evolution of topics in education research: a systematic review using bibliometric analysis, *Educ. Rev.* 72 (3) (2020) 281–297.
- [41] R. Raman, V.K. Nair, V. Prakash, A. Patwardhan, P. Nedungadi, Green-hydrogen research: what have we achieved, and where are we going? *Bibliometrics analysis, Energy Rep.* 8 (2022) 9242–9260.
- [42] K. Achuthan, V.K. Nair, R. Kowalski, S. Ramanathan, R. Raman, Cyberbullying research—alignment to sustainable development and impact of COVID-19: bibliometrics and science mapping analysis, *Comput. Hum. Behav.* 140 (2023), 107566.
- [43] V. Vziatysheva, Determinants of individuals’ belief in fake news: a scoping review determinants of belief in fake news, *PLoS One* 16 (6) (2021), e0253717.
- [44] A. Nasir, K. Shaukat, K.I. Khan, I.A. Hameed, T.M. Alam, S. Luo, What is core and what future holds for blockchain technologies and cryptocurrencies: a bibliometric analysis, *IEEE Access* 9 (2020) 989–1004.
- [45] A.V. Shvets, D.A. Devyatkin, I.V. Smirnov, I.A. Tikhomirov, K.V. Popov, K.N. Yarygin, The study of systems and methods for scientometric analysis of scientific publications, *Sci. Tech. Inf. Process.* 42 (2015) 359–366.
- [46] N.J. Van Eck, L. Waltman, Citation-based clustering of publications using CitNetExplorer and VOSviewer, *Scientometrics* 111 (2017) 1053–1070.
- [47] L. Waltman, N.J. Van Eck, E.C. Noyons, A unified approach to mapping and clustering of bibliometric networks, *Journal of informetrics* 4 (4) (2010) 629–635.
- [48] L. Cardoso, R. Silva, G.G.F.D. Almeida, L. Lima Santos, A bibliometric model to analyze country research performance: SciVal topic prominence approach in tourism, leisure and hospitality, *Sustainability* 12 (23) (2020) 9897.
- [49] P. Booth, S.A. Chaperon, J.S. Kennell, A.M. Morrison, Entrepreneurship in island contexts: a systematic review of the tourism and hospitality literature, *Int. J. Hospit. Manag.* 85 (2020), 102438.
- [50] R. Raman, V.K. Nair, A. Shivdas, R. Bhukya, P.K. Viswanathan, N. Subramaniam, P. Nedungadi, Mapping Sustainability Reporting Research with the UN’s Sustainable Development Goal, *Heliyon*, 2023.
- [51] R. Raman, N. Subramaniam, V.K. Nair, A. Shivdas, K. Achuthan, P. Nedungadi, Women entrepreneurship and sustainable development: bibliometric analysis and emerging research trends, *Sustainability* 14 (15) (2022) 9160.
- [52] L. Leydesdorff, The global structure of scientific collaboration, *Journal of the Association for Information Science and Technology* 70 (3) (2019) 333–351.
- [53] X. Li, L. Lei, A bibliometric analysis of topic modelling studies (2000–2017), *J. Inf. Sci.* 47 (2) (2021) 161–175.
- [54] S. Chaudhary, A. McGregor, D. Houston, N. Chettri, The evolution of ecosystem services: a time series and discourse-centered analysis, *Environ. Sci. Pol.* 54 (2015) 25–34.
- [55] A. Lis, Keywords co-occurrence analysis of research on sustainable enterprise and sustainable organization, *Journal of Corporate Responsibility and Leadership* 5 (2) (2018) 47–66.
- [56] S. Lozano, L. Calzada-Infante, B. Adenso-Díaz, S. García, Complex network analysis of keywords co-occurrence in the recent efficiency analysis literature, *Scientometrics* 120 (2019) 609–629.
- [57] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, M. Karir, Taming the 800 pound gorilla: the rise and decline of NTP DDoS attacks, in: *Proceedings of the 2014 Conference on Internet Measurement Conference, 2014*, pp. 435–448.
- [58] C. Pachkha, M. Debbabi, Darknet as a source of cyber intelligence: survey, taxonomy, and characterization, *IEEE Communications Surveys & Tutorials* 18 (2) (2015) 1197–1227.
- [59] M.W. Al Nabki, E. Fidalgo, E. Alegre, I. De Paz, Classifying illegal activities on tor network based on web textual contents, in: *Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics, 1*, Long Papers, 2017, pp. 35–43.
- [60] M. Tzanetakis, G. Kamphausen, B. Werse, R. von Laufenberg, The transparency paradox. Building trust, resolving disputes and optimizing logistics on conventional and online drugs markets, *Int. J. Drug Pol.* 35 (2016) 58–68.
- [61] F. Thomaz, C. Salge, E. Karahanna, J. Hulland, Learning from the Dark Web: leveraging conversational agents in the era of hyper-privacy to enhance marketing, *J. Acad. Market. Sci.* 48 (2020) 43–63.
- [62] F. Wehinger, The dark net: self-regulation dynamics of illegal online markets for identities and related services, in: *2011 European Intelligence and Security Informatics Conference, IEEE, 2011*, pp. 209–213.
- [63] A. Montieri, D. Ciunozzo, G. Aceto, A. Pescapé, Anonymity services tor, I2P, JonDonym: classifying in the dark (web), in: *IEEE Transactions on Dependable and Secure Computing*, 17, 2020, pp. 662–675, <https://doi.org/10.1109/TDSC.2018.2804394>, no. 3.
- [64] J. Dalins, C. Wilson, M. Carman, Criminal motivation on the Darkweb: a categorization model for law enforcement, *Digit. Invest.* 24 (2018) 62–71.
- [65] A. Bancroft, P.S. Reid, Concepts of illicit drug quality among Darknet market users: purity, embodied experience, craft and chemical knowledge, *Int. J. Drug Pol.* 35 (2016) 42–49.
- [66] J. Brošćus, D. Rhumorbarbe, C. Mireault, V. Ouellette, F. Crispino, D. Décarry-Héту, Studying illicit drug trafficking on Darknet markets: structure and organization from a Canadian perspective, *Forensic Sci. Int.* 264 (2016) 7–14.
- [67] A. Maddox, M.J. Barratt, M. Allen, S. Lenton, Constructive activism in the Darkweb: cryptomarkets and illicit drugs in the digital ‘demimonde’, *Inf. Commun. Soc.* 19 (1) (2016) 111–126.
- [68] E. Duchemin, The Darkweb: a breeding ground for COVID-19 misinformation, *European Journal of Risk Regulation* 11 (3) (2020) 331–333.
- [69] J.H. Bates, D.G. Fiebig, C. Piesse, N. Wille, COVID-19 misinformation on the Darkweb: a preliminary analysis, *Health Security* 18 (5) (2020) 521–528.
- [70] R. Van Wegberg, J.J. Oerlemans, O. van Deventer, Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin, *J. Financ. Crime* (2018).
- [71] H. Kuzuno, C. Karam, Blockchain explorer: an analytical process and investigation environment for bitcoin, in: *2017 APWG Symposium on Electronic Crime Research (eCrime)*, IEEE, 2017, pp. 9–16.
- [72] H.T. Wu, C.W. Tsai, An intelligent agriculture network security system based on private blockchains, *J. Commun. Network.* 21 (5) (2019) 503–508.
- [73] D. Seyler, W. Liu, Y. Zhang, X. Wang, C. Zhai, Darkjargon. net: a platform for understanding underground conversation with latent meaning, in: *Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval, 2021*, pp. 2526–2530.
- [74] P. Evangelatos, C. Iliou, T. Mavropoulos, K. Apostolou, T. Tsikrika, S. Vrochidis, I. Kompatsiaris, Named entity recognition in cyber threat intelligence using transformer-based models, in: *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, IEEE, 2021, pp. 348–353.
- [75] J. Bogensperger, S. Schlarb, A. Hanbury, G. Recksi, DreamDrug-A crowdsourced NER dataset for detecting drugs in Darknet markets, in: *Proceedings of the Seventh Workshop on Noisy User-Generated Text, W-NUT 2021, 2021*, pp. 137–157.
- [76] S. Kethineni, Y. Cao, C. Dodge, Use of bitcoin in Darknet markets: examining facilitative factors on bitcoin-related crimes, *Am. J. Crim. Justice* 43 (2018) 141–157.
- [77] P. Seele, Let us not forget: crypto means secret. Cryptocurrencies as enabler of unethical and illegal business and the question of regulation, *Humanistic Management Journal* 3 (1) (2018) 133–139.
- [78] P. Marmora, Currency substitution in the shadow economy: international panel evidence using local Bitcoin trade volume, *Econ. Lett.* 205 (2021), 109926.

- [79] X. Jie, L. Haoliang, J. Ao, A new model for simultaneous detection of phishing and Darknet websites, in: 2021 7th International Conference on Computer and Communications (ICCC), IEEE, 2021, pp. 2002–2006.
- [80] I.N.V.D. Naveen, K. Manamohana, R. Verma, Detection of malicious URLs using machine learning techniques, *Int. J. Innovative Technol. Explor. Eng.* 8 (4S2) (2019) 389–393.
- [81] Z. Guo, Y. Guan, Active probing-based schemes and data analytics for investigating malicious fast-flux web-cloaking based domains, in: 2018 27th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2018, pp. 1–9.
- [82] A. Dainotti, A. King, K.C. Claffy, F. Papale, A. Pescapé, Analysis of a"/0" stealth scan from a botnet, in: Proceedings of the 2012 Internet Measurement Conference, 2012, pp. 1–14.
- [83] M.W. Al-Nabki, E. Fidalgo, E. Alegre, L. Fernández-Robles, Torank: identifying the most influential suspicious domains in the tor network, *Expert Syst. Appl.* 123 (2019) 212–226.
- [84] T. Ban, L. Zhu, J. Shimamura, S. Pang, D. Inoue, K. Nakao, Detection of botnet activities through the lens of a large-scale Darknet, in: Neural Information Processing: 24th International Conference, ICONIP 2017, 2017.
- [85] M. Pannu, I. Kay, D. Harris, Using Darkweb crawler to uncover suspicious and malicious websites, in: Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21–25, 2018, Loews Sapphire Falls Resort at Universal Studios, 9, Springer International Publishing, Orlando, Florida, USA, 2019, pp. 108–115.
- [86] T.N. van Leeuwen, R.J.W. Tijssen, M.S. Visser, *Bibliometrics and Research Evaluation: A Practical Guide*, Cambridge University Press, 2014.
- [87] L. Bornmann, R. Mutz, H.D. Daniel, What do citation counts measure? A review of studies on citing behavior, *Journal of the Association for Information Science and Technology* 66 (2) (2015) 243–269.
- [88] L. Waltman, N.J. van Eck, B. van der Meulen, A tutorial on network analysis of scientific publications, *Scientometrics* 106 (3) (2016) 689–702.
- [89] R. Van Noorden, Beyond the impact factor, *Nature* 515 (7525) (2014) 461–463.