International Journal of Electrical Engineering and Intelligent Computing (IJEEIC) EISSN 3031-5255
https://ejournal.unkhair.ac.id/index.php/ijeeic/index

Analyzing Illegal Trade On The Dark Web

Zaid Mundher
Department of Computer Science/ University of Mosul/ Mosul - Iraq
*zaidabdulelah@gmail.com

Article history : Received October 13, 2025 | Revised Desember 30, 2025 | Accepted January 4, 2026

Internet can be divided, in terms of accessibility, into three main categories: Surface web, Deep web, and Dark web. The dark part is considered the most dangerous of these types due to the difficulty of tracking its users and the anonymity it offers, making it widely used for illegal activities. This research aims to measure the prevalence of illegal activities in Iraq and some neighboring countries, specifically Syria, Saudi Arabia, and Iran. The activities tracked include: drug trafficking, fake documents, and weapons trafficking. The search engine "Ahmia" was used to collect dark web links (with the .onion extension) as an initial stage. In the second stage, the Tor network was used to access these links to obtain more information from each page. A dataset of approximately 5,000 pages was created and analyzed to generate a set of insights related to the data. The results showed that Iraq appears more prominently compared to neighboring countries, reflecting the widespread use of dark web sites, as will be discussed later in this work.

Keywords: Dark We, Cybercrime,Tor Network, Ahmia Search Engine, Community.

1. INTRODUCTION

The internet, as the general public knows it, is a collection of websites used daily, in addition to the services available for one benefit or another. However, the websites that are openly used and the services that are publicly available are only part of a larger environment and broader services that are not visible in their natural form. There is another part of the internet that is not visible to the majority, and many Internet users may not even know about it: the dark web. Dark web is the hidden part of the Internet that is not indexed by search engines and cannot be accessed using known search engines such as Google, nor can its sites be accessed using regular browsers such as Chrome. It is a completely separate world with its own tools and methods [1][2][3][4]. Although the dark web was initially intended for good purposes, and it still has legitimate uses—such as enabling freedom of expression in repressive regimes—it has also become a center for illegal activities, taking advantage of the anonymity and untraceability afforded to its users[5][6]. Despite the challenges of tracking, tracing, and identifying users, understanding how the dark web works is critical for researchers, law enforcement officials, and cyber-security experts. This work introduces a case study of Iraq, in addition to its neighboring countries—specifically Syria, Saudi Arabia, and Iran, seeking to answer several key questions, such as:

- What is the frequency of Iraq's appearance on the dark web?
- What are the most common types of illicit activities on the dark web in the countries under study?
- What is the contact information (such as email addresses or Telegram IDs) of illegal promoters, as shown in the retrieved pages?

To answer the above questions, a series of steps were completed, from collection to analysis. The first step was using Ahmia search engine, which is a privacy-preserving search engine that combs hidden-service sites on the Tor network and can index .onion sites on the dark web [7]. Tor network (The Onion Router) is an anonymous Internet where its traffic goes through multiple encrypted proxy relay [8]. For browsing automation and for accurate data extraction, we used the Selenium library, which helped us to handle dynamic pages and obviate crawling problems. Handling the results, graph technique was used to represent the data where vendors, marketplaces, and contact points were represented as nodes and their relations as edges. Community detection was also addressed in this work using the Louvain modularity [9]. Collectively, these techniques formed a pipeline that introduce complete steps to gather, store, process, and investigate dark web data.

The main aim of this work is to introduce an analytical perspective on the dark web activities by combining data collection, network analysis, and community detection methods to provide a better understanding of regional illicit online behavior.

Research on the dark web has expanded significantly in recent years, ranging from general studies to those specialized in illicit markets, as well as work focused on discovering criminal communities through network analysis. Existing work can be classified into several main areas:

First: General studies on the dark web and cybercrime:

A number of studies have provided comprehensive reviews of the general structure of the dark web, its anonymity mechanisms, and the difficulties associated with monitoring illicit activities. Authors in [1],[2] and [3] addressed the evolution of threats on the dark web, anonymity mechanisms, and monitoring methods. In contrast, Authors in [6] and [10] also discussed issues related to threat detection, cyber-security, and the challenges facing security agencies. These studies agree that the dark web is a dual-use platform, exploited for both legitimate and illicit purposes.

Second: Studies on illicit markets and crypto-markets.

Another part of work has focused on analyzing online black markets, particularly those related to drug trafficking. For example, [7] studied the infamous Silk Road market, while authors of [14] examined the chronological evolution of anonymous markets. Moreover, authors of [9][10] discussed the characteristics of drug markets, while authors of [11] revealed the role of online markets in spreading drug trafficking. Work of [8] examined recent trends related to crypto-currencies in drug trafficking. Together, these studies shed light on how patterns of illicit online trade have emerged and evolved.

Third: Emerging trends and recent contextual studies.

Other research has demonstrated how dark web activity is influenced by global and technological developments. For example, authors of [16] examined black market activity during the COVID-19 pandemic, while work of [5] focused on future trends in cybercrime, and [17] proposed a new forensic protocol (D2WFP) for analyzing browsing activity on the dark web. Work of [18] presented a bibliometric study linking dark web research to the United Nations Sustainable Development Goals. Furthermore, authors of [19] analyzed the misuse of cryptocurrencies on the dark web, uncovering large-scale illicit campaigns. These works illustrate the dynamic and adaptive nature of illicit markets.

Fourth: Community discovery and network analysis.

Another group of studies has addressed the organizational structure of criminal groups using community discovery techniques. In [20], a bipartite model was proposed to detect hidden connections between criminals, while [21] introduced the HICODE framework to detect hidden communities alongside dominant ones, and authors of [22] reviewed recent developments in community discovery using deep learning techniques. These methodological works emphasize the importance of combining structure and attributes to detect overlapping or latent communities, which directly intersects with our study.

Although previous studies have provided important insights at the global level, few have focused on the Middle East. Therefore, this research contributes to filling this gap by presenting a case study of Iraq and neighboring countries, relying on Ahmia crawling and Tor network, network analysis, and community discovery techniques to understand the nature of illicit markets in this understudied region.

2. METHOD

Practically, this work can be divided into sequential steps. It begins with collecting data from Iraq and its neighboring countries, followed by analyzing the data to generate meaningful insights. The general process starts with a surface-level search for dark web links containing specific keywords related to Iraq and its neighbors, then proceeds with a deep crawl through the Tor network to extract additional information and metadata for each link. Once the data is collected, it is cleaned and pre-processed, after which an analysis is performed to derive insights and perspectives. The stages are detailed below.

2.1 Search and Data Collection

At this stage, a list of keywords to be searched for, was created, as shown in Table 1. The search was conducted using the Ahmia search engine. A total of 4,383 unique URLs with the extension ".onion" were extracted. These links will be used in the second stage to access dark web sites.

Table 1. Search Keywords

Country	Search Terms
Iraq	iraq drugs, iraq fake id, iraq weapons
Syria	syria drugs, syria fake id, syria weapons
Iran	iran drugs, iran fake id, iran weapons
Saudi Arabia	saudi arabia drugs, saudi arabia fake id, saudi arabia weapons

2.2 Crawling and Metadata Extraction

Using the Tor Expert Bundle, each URL was accessed programmatically to extract the following information:

- Page title

- Contact information (Telegram, email, phone)
- Country names

To avoid being blocked, a 10-second delay was introduced between each request. Overall, the extraction process took approximately 50 hours to go through all the links and retrieve the necessary data. The following key attributes (Table 2) were extracted from the collected web pages.

Table 2. Extracted Attributes from Collected Web Pages

Attribute	Description
Title	HTML page title
Search_Keyword	Keyword used
Has_Contact	Contact info flag
Telegram_Handles	Extracted Telegram IDs
Email_Addresses	Extracted emails
Phone_Numbers	Extracted phone numbers
Country	Identified country
Error	Connection/parsing issues

2.3 Data Cleaning

After completing data collection, the dataset was cleaned and pre-processed to remove broken links, duplicate entries, and pages that were inaccessible for various reasons.

2.4 Exploratory Analysis

Various exploratory analyses were performed from simple statistics, co-occurrence checks and network visualizations. One effort centered on monitoring contact names — Telegram user handles, in particular — to spot behaviors that might indicate vendor hubs or criminal clusters. It allowed us to do analysis on the network and community detection, which helped in better understanding of connections between actors and listings in the dark web.

2.5 Challenges and Limitations

This study had a certain number of technical and practical limitations, which we experienced during the course of this study:

- Unavailable Pages: A significant number of .onion links could not be reached—either because the servers were offline, or because the sites actively blocked automated crawlers. These cases were logged using an error flag and excluded from the main analysis.
- Dynamic Web Content: Some dark web websites use JavaScript which needs a specific processing. Selenium library was used to handle this issue. However, this increased the total crawling time and complexity.
- Language Diversity: Although most collected pages were in English, we faced pages written in Arabic and Persian. As a result, some local data may not be fully represented.
- Ethical Boundaries: Ethical and legal boundaries were adhered to, as we did not involve to any illegal transactions. Overall, this study relied only on observation.
- Sampling Bias: Relying on Ahmia as our primary search tool means we only captured a part of the dark web. Because Ahmia does not index all .onion sites, there may have been some content related to the search topic that we missed.

Despite these limitations, the collected dataset remained rich enough to allow meaningful patterns to emerge—particularly when combined with network analysis and community detection techniques.

3. RESULTS

The final dataset has 4,983 .onion links related to illegal activities, collected through keyword-based searches using Ahmia. Fig. 1 shows a sample of the collected data of phase 1, while Fig. 2 shows a sample data of phase 2.

	Search_Keyword	Country	URL
0	iraq drugs	Iraq	http://bellcatmbguthn3age23lrbseln2lryzv3mt7wh...
1	iraq drugs	Iraq	http://qi3efcj4jv4ncv66irsoh7shukkyy4bqrlaccq4...
2	iraq drugs	Iraq	http://6jtzh4syyeizyfzodzvelw5a6ro2tjn66bwo6yg...
3	iraq drugs	Iraq	http://6jtzh4syzechfgzkaeoxbxvtl3pekm4pfpg54jl...
4	iraq drugs	Iraq	http://bg3phk4asaa5urdgg74ui2nkawucidvxxt6g4ow...

Figure 1. Sample Data of Phase 1

	Search_Keyword	Country	URL	Title	Has_Contact	Telegram_Handles	Email_Addresses
0	iraq drugs	Iraq	http://bellcatmbguthn3age2...	Iraq - bellingcat	No	[]	[]
1	iraq drugs	Iraq	http://qi3efcj4jv4ncv66irs...	Iraq Driver License - Iraq...	Yes	['@realfakesonline']	['contact@realfakesonline....
2	iraq drugs	Iraq	http://6jtzh4syyeizyfzodzv...	Buy guns in Iraq Archives ...	Yes	['@grandarms', '@grandarms...	[]
3	iraq drugs	Iraq	http://6jtzh4syzechfgzkaeo...	Buy guns in Iraq Archives ...	Yes	['@grandarms', '@grandarms...	[]
4	iraq drugs	Iraq	http://bg3phk4asaa5urdgg74...	Buy Ketamine in Iraq Archi...	Yes	['@Hoffmanncrewofficial', ...	[]

Figure 2. Sample Data of Phase 2

Different visualizations were made to help with data analysis by giving more information about the search activity and the linkages between them. Fig. 3 shows how many searches were done by country, which makes it easy to see which areas had the most user activity on the platform being studied. Fig. 4 shows the most common search phrases which can help to understand what people are most interested in and how they behave. In addition, Fig. 5 displays the number of URLs that were accessed, broken down by nation. These three graphs together illustrate that there is a big difference in how many countries are mentioned in different regions. The fact that Iraq is so common on these lists shows that it could be both a target market and a place where goods are moved or stored.

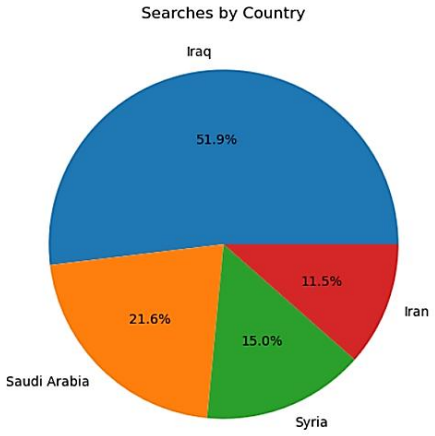

Figure 3. Number of Searches Conducted by Country

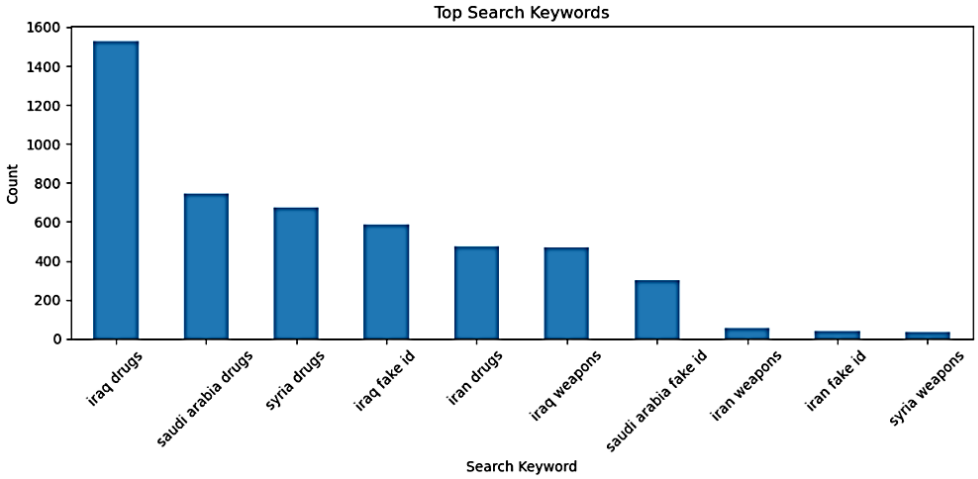

Figure 4. Most Common Search Phrases in the Dataset

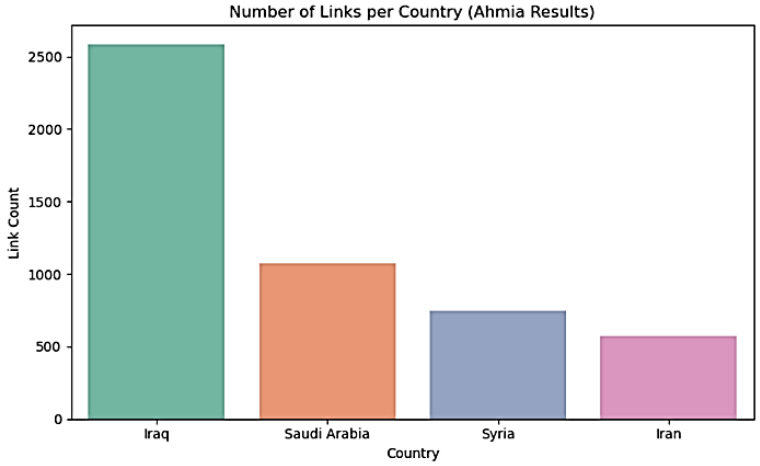

Figure 5. Number of Accessed .onion URLs by Country

As addition analyze, using a rule-based classifier on page titles and URLs, pages were categorized into five groups as displayed in Fig. 6. As easily noticeable in the chart, the number of drug-related topics far exceeds the number of topics related to weapons and counterfeit papers.

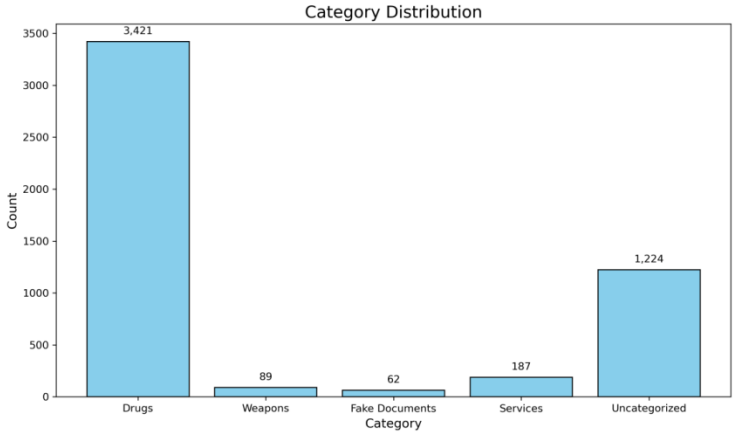

Figure 6. Categorization of Pages by Topic

Also, a word cloud generated from page titles (Fig. 7) was used to capture the most frequent textual patterns and highlight dominant themes or keywords across the dataset. This helps to understand the semantic focus of the crawled content.

Figure 7. Word Cloud of Page Titles Highlighting Frequent Terms

Communication handles were extracted and counted in this step. Telegram emerged as the dominant platform for contact, particularly in drug-related listings. Some handles were reused across several pages, possibly indicating repeat vendors or organized seller groups. Fig. 8 illustrates the number of pages containing direct contact details such as email addresses, phone numbers, or Telegram handles, thereby indicating the extent of reachable entities within the collected dataset.

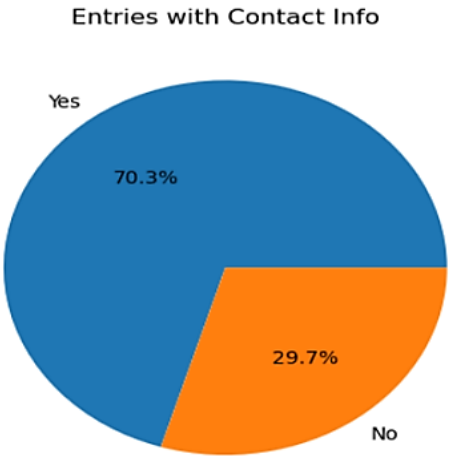

Figure 8. Number of Pages Containing Direct Contact Information

Also, two lists were made to show the most common contact information: Top 10 Telegram Handles (Fig. 9) and Top 10 Email Addresses (Fig. 10). These lists give a better look at possibly active entities or recurring identifiers in the market.

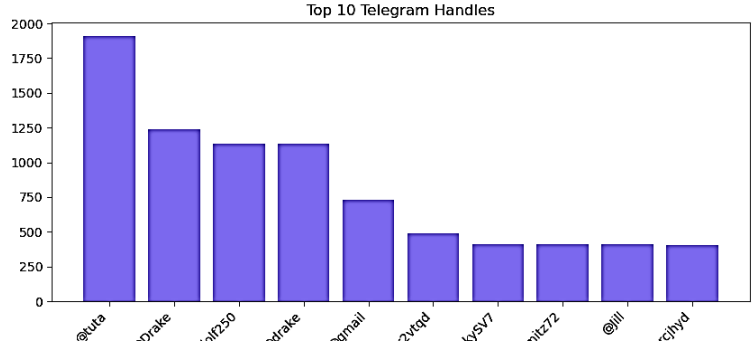

Figure 9. Top 10 Most Frequent Telegram Handles

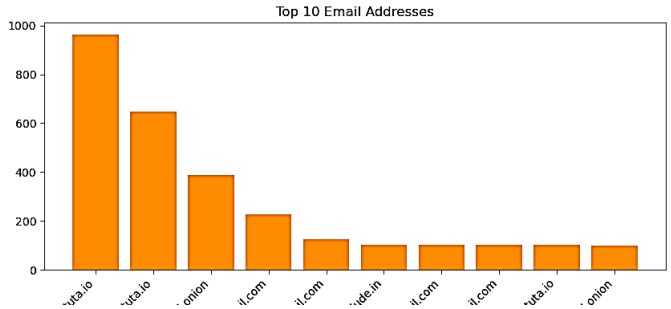

Figure 10. Top 10 Most Frequent Email Addresses

A complete contact-based network graph was created to look into the structure and connections between dark web listings and the ways they communicate with each other (Fig. 11). In this network: Nodes represent either .onion service pages or extracted contact elements, including Telegram handles and email addresses. Edges link contact nodes to the sites where they show up, making it possible to find handles that are used in more than one listing.

The presented network in Fig. 11 has more than 400 nodes and hundreds of edges. It shows both isolated actors and communities that are well connected. The contact nodes were color-coded by type: gray for pages, blue for Telegram handles, and orange for emails. The size of a node shows how many connections it has, which makes it easy to find contacts that are often referenced.

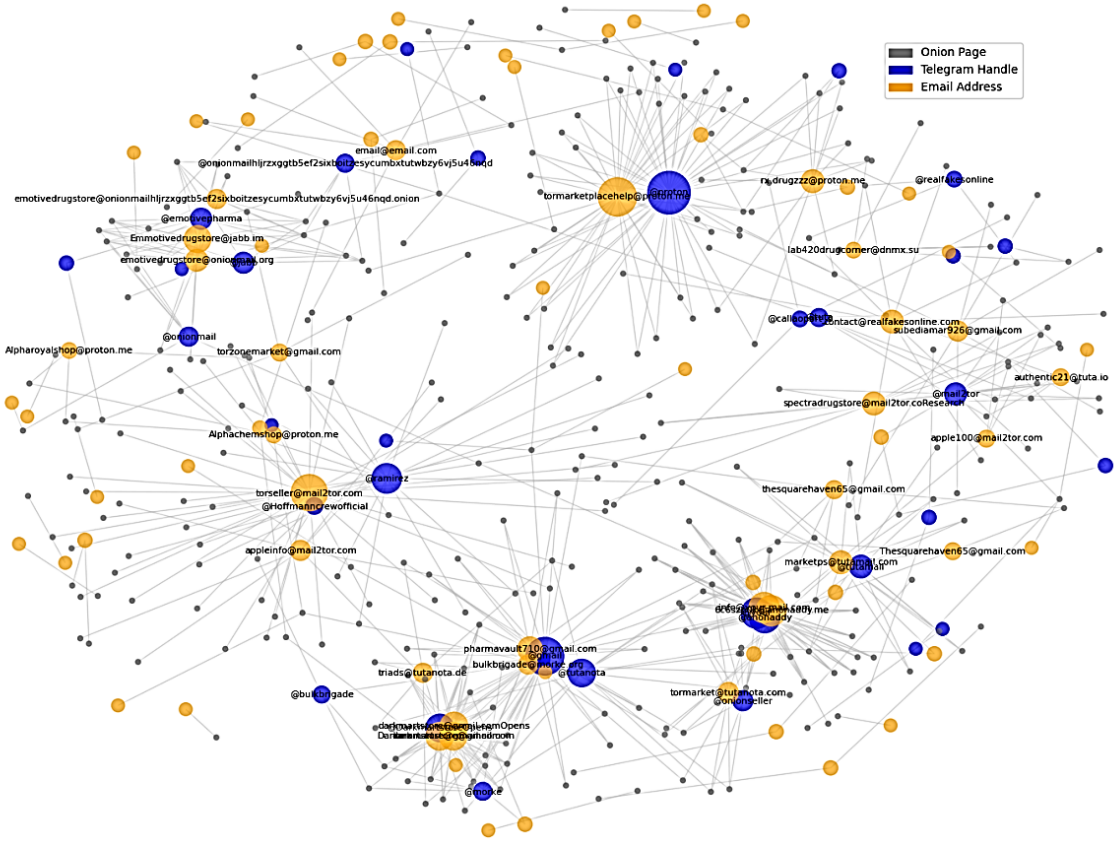

Figure11. Contact Network Graph Linking Dark Web Pages and Communication Handles

The network of contacts explains patterns of contact reuse. For example, the node marketpiecehelp@protonmail.com appears in numerous listings across multiple communities. Its high centrality suggests it may act as a market administrator or support center. The presence of such nodes reflects coordination mechanisms in dark web marketplaces, potentially pointing to organized vendor networks or centralized platforms. Another point to note is that a name of @callaoport_1, was observed in more than a dozen listings,

suggesting they function as bridges between multiple categories such as drugs and fake documents.

On the other hand, with the use of the Louvain modularity method, we were able to uncover more than 50 different communities and learn more about their structure. There are .onion pages and contact handles in each community that are more connected to each other than to the rest of the network. Some of the most significant communities are mentioned in Table 3:

Table 3. Summary of Most Significant Communities Identified via Louvain Modularity

Community ID	Total Nodes	Pages (.onion)	Contact Handles
30	47	44	3
18	42	33	9
13	30	20	10
8	31	30	1
0	12	10	2

These community-level may be explained as follows:
Community 30: A limited group of connections is used on several pages. This could mean that there is a single seller or market aggregator.
Community 13: The fact that so many individuals are contacting pages demonstrates that a lot of services are working together and using the same strategies.
Community 8: There are a lot of postings connected to one contact, which makes it look like a catalog or hub service.

4. DISCUSSION

The analysis of dark web data related to Iraq and its neighboring countries has revealed several important patterns that shed light on the structure and behavior of regional illicit markets online.
Iraq stood out in the dataset with a large number of listings and frequent keyword appearances. Many of these listings targeted Iraqi users directly (e.g., “Buy cocaine in Iraq”), while others suggest that Iraq might be used as a transit or distribution point for illegal goods. The repeated use of Iraq-related terms alongside keywords like *“buy”, “online”,* and various drugs points to strong demand.

Many advertisements included contact details such as WhatsApp numbers, email addresses, or Telegram identities. For the majority of suppliers, Telegram is usually the preferred platform where listed more than once. This suggests that some vendors are active in more than one marketplace or even category. This is further supported by our network analysis, which found clusters of related vendors and linked pages with similar contact handles. These trends suggest that dark web activity often involves organized vendor collectives or market aggregators, rather than being completely isolated or random.

Timeouts, unavailable domains, or server issues caused about 18% of the links in the dataset to fail to load. The ecosystem is very unstable because marketplaces often switch domains or go offline to avoid detection making the data collection process is challenging. To address some of these issues, Tor Expert Bundle, SOCKS proxies, and headless browsers were used to keep servers from getting blocked or overloaded. This also required lengthy processing times and strict security measures.

Dealing with illegal market online has serious ethical issues. This research followed a passive approach that does not include any interact with vendors, make purchases, or attempt to access restricted content. All data was collected from publicly available search results. The ultimate goal of this work is to support policy-makers, cybersecurity experts, and researchers in understanding regional darknet threats—not to expose individuals or promote any form of illicit activity. These insights emphasize the value of graph-based analysis for understanding hidden relationships in dark web data and can guide cyber threat intelligence efforts focused on the Middle East.

5. CONCLUSION

This study investigate dark web data that related to Iraq and its neighboring countries (Syria, Iran, and Saudi Arabia), focusing on illicit activities such as drug transfer, fake ID distribution, and weapon sales. Search queries on the Ahmia engine were implemented to collect data. A dataset of nearly 5,000 listings with metadata such as page titles, contact methods, and country mentions was successfully gathered. Our results show that Iraq

is frequently mentioned in these listings—far more than neighboring countries—suggesting its significance as a target market, a transit point, or both. Results have also shown that most of the collected data were related to drugs, but some also involved other forms of illegal activities. Telegram emerged as the dominant method of contact, highlighting its popularity among dark web vendors. An important finding of this study relates to network and community analysis. By linking pages to contact IDs, groups of lists were revealed that were likely run by the same individuals or coordinated networks. These findings help identify the most active actors on the dark web, enabling digital forensics efforts to be directed toward these individuals. Furthermore, during the work phases, we noted technical limitations in dealing with .onion sites, some of which are unstable and frequently updated. Language differences posed another challenge—although most of the content was in English, some lists used Arabic or translated text, preventing access to complete data on the topic. Future research may include Arabic language detection and multilingual crawling to improve regional accuracy.

This study represents a first step that the Iraqi government can use to determine the extent of the dark web's use in illegal activities, relying on quantitative indicators and actual numbers. This research can be considered a starting point to increase attention to this area, which will contribute—directly or indirectly—to curbing the expansion of dark web sites in illegal activities.

REFERENCES

[1] M. K. Alshammery and A. F. Aljuboori, "Crawling and Mining the Dark Web: A Survey on Existing and New Approaches," *Iraqi Journal of Science*, vol. 63, no. 3, pp. 265–288, Mar. 2022, doi: 10.24996/ijs.2022.63.3.36.

[2] J. Saleem, R. Islam, and M. A. Kabir, "The Anonymity of the Dark Web: A Survey," *IEEE Access*, vol. 10, pp. 1–1, Jan. 2022, doi: 10.1109/ACCESS.2022.3161547.

[3] S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan, "Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach," *IEEE Access*, vol. 8, pp. 171796–171819, Jan. 2020, doi: 10.1109/ACCESS.2020.3024198.

[4] M. A. Alotaibi, M. A. AlZain, M. Masud, and J. Al-Amri, "Computer Forensics: Dark Net Forensic Framework and Tools Used for Digital Evidence Detection," *International Journal of Communication Networks and Information Security*, vol. 11, no. 3, Dec. 2019, doi: 10.17762/ijcnis.v11i3.4407.

[5] S. Temara, "The Dark Web and Cybercrime: Identifying Threats and Anticipating Emerging Trends," *International Journal of Advanced Engineering Research and Science*, vol. 11, no. 10, pp. 80–93, Oct. 2024, doi: 10.22161/ijaers.1110.8.

[6] I. Mahmood, M. Rahman, and M. A. Rahman, "A Survey on Dark Web Monitoring and Corresponding Threat Detection," 2022.

[7] Ahmia.fi, "Ahmia Search Engine," 2014. [Online]. Available: https://ahmia.fi/. [Accessed: Aug. 20, 2025].

[8] The Tor Project, "Tor Protocol Specifications," 2023. [Online]. Available: https://spec.torproject.org/. [Accessed: Aug. 20, 2025].

[9] B. Yao, J. Zhu, P. Ma, K. Gao, and X. Ren, "A Constrained Louvain Algorithm with a Novel Modularity," *Applied Sciences*, vol. 13, no. 4045, 2023, doi: 10.3390/app13064045.

[10] R. Saha, "Cybersecurity and the Dark Web," *International Journal of Research Publication and Reviews*, vol. 5, no. 3, pp. 2742–2746, Mar. 2024.

[11] K. Soska and N. Christin, "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem," in *Proc. 24th USENIX Security Symposium*, Washington, D.C., USA, 2015, pp. 33–48.

[12] M. Tzanetakis, "Online drug distribution: alternatives to physical violence in conflict resolution," 2015, doi: 10.25365/phaidra.59.

[13] M. Tzanetakis, "Comparing cryptomarkets for drugs: A characterisation of sellers and buyers over time," *International Journal of Drug Policy*, vol. 56, pp. 176–186, Jun. 2018, doi: 10.1016/j.drugpo.2018.01.022.

[14] J. Aldridge and D. Décary-Hétu, "Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets," *International Journal of Drug Policy*, vol. 35, pp. 7–15, May 2016, doi: 10.1016/j.drugpo.2016.04.020.

[15] J. Sasikumar, "Dark Net Drug Transactions (DNDT): An Emerging Cryptotrend in Drug Trafficking," *Indian Journal of Criminology*, vol. 51, no. 1, 2023.

[16] A. Bracci, M. Nadini, M. Aliapoulios, D. McCoy, I. Gray, A. Teytelboym, A. Gallo, and A. Baronchelli, "Dark Web Marketplaces and COVID-19: Before the Vaccine," *EPJ Data Science*, vol. 10, no. 1, Dec. 2021, doi: 10.1140/epjds/s13688-021-00259-w.

[17] M. C. Ghanem, P. Mulvihill, K. Ouazzane, R. Djemai, and D. Dunsin, "D2WFP: A Novel Protocol for Forensically Identifying, Extracting, and Analysing Deep and Dark Web Browsing Activities," *Journal of Cybersecurity and Privacy*, vol. 3, no. 4, pp. 808–829, Nov. 2023, doi: 10.3390/jcp3040036.
[18] R. Raman, V. Nair, P. Nedungadi, I. Ray, and K. Achuthan, "Darkweb Research: Past, Present, and Future Trends and Mapping to Sustainable Development Goals," *Heliyon*, vol. 9, no. 9, e22269, Sep. 2023, doi: 10.1016/j.heliyon.2023.e22269.
[19] P. Xia, Z. Yu, K. Wang, K. Ma, S. Chen, X. Luo, Y. Zhou, L. Wu, and G. Bai, "The Devil Behind the Mirror: Tracking the Campaigns of Cryptocurrency Abuses on the Dark Web," *arXiv preprint*, arXiv:2401.04662, Jan. 2024, doi: 10.48550/arXiv.2401.04662.
[20] H. Isah, C. Neagu, and P. Trundle, "A Bipartite Network Model for Inferring Hidden Ties in Crime Data," *arXiv preprint*, arXiv:1510.02343, Oct. 2015.
[21] K. He, Y. Li, S. Soundarajan, and J. Hopcroft, "Hidden Community Detection in Social Networks," *Information Sciences*, vol. 425, pp. 92–106, 2018, doi: 10.1016/j.ins.2017.10.019.
[22] X. Su, S. Xue, F. Liu, J. Wu, J. Yang, C. Zhou, W. Hu, C. Paris, S. Nepal, D. Jin, Q. Sheng, and P. Yu, "A Comprehensive Survey on Community Detection With Deep Learning," *IEEE Transactions on Neural Networks and Learning Systems*, early access, pp. 1–21, 2022, doi: