Journal of Theoretical and Applied Information Technology
31st May 2023. Vol.101. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HOW DARK WEB MONITORING CAN BE USED FOR OSINT AND INVESTIGATIONS

ALANOUD ALQUWAYZANI[1], RAWABI ALDOSSRI[1], and M M HAFIZUR RAHMAN[2]

Dep of Computer Networks and Communications, CCSIT, King Faisal University, Al Hassa 31982, Saudi Arabia Email: [1]222402679@student.kfu.edu.sa, [2]222400163@student.kfu.edu.sa, [3]mhrahman@kfu.edu.sa

ABSTRACT

The dark web is a hidden network of websites that cannot be accessed through regular search engines or browsers. It is often associated with illegal activities, such as the sale of illicit goods and services, human trafficking, and other criminal activities. Despite its illicit reputation, the dark web contains a wealth of information that can be utilized for open-source intelligence (OSINT) and investigations. This article explores how dark web monitoring can be utilized for OSINT and investigations. It discusses the ways in which dark web monitoring can be used to identify and track illegal activities on the dark web. Specifically, it examines the sale of illegal goods and services, the distribution of prohibited content, and the planning of criminal activities. By monitoring the dark web, law enforcement and security professionals can gain valuable insights into criminal activities and take appropriate action to prevent or mitigate them. However, dark web monitoring presents several challenges and limitations. The biggest challenge is the need for specialized knowledge and technical expertise to navigate the dark web safely and effectively. In addition, there is a risk of exposure to potentially harmful or illegal content, which can pose a risk to individuals or organizations who are not well-versed in the intricacies of the dark web. Overall, this article provides insights into the potential of dark web monitoring for OSINT and investigations. It emphasizes the need for caution and specialized knowledge to ensure that individuals and organizations can navigate the dark web safely and effectively. With the proper tools and expertise, dark web monitoring can be powerful for gathering intelligence and combating criminal activities.

Keywords: *Dark* Web, open-source intelligence, Investigation, Digital crime, cybercrime.

1. INTRODUCTION

Recent scrutiny of surface web activities appears to be driving an influx of new users, including illicit goods sellers, to the dark web, which has gained widespread notoriety in recent years. Now that it has been established, it functions as a segment of the internet where criminal networks can operate more freely and terrorist networks can keep their communications safe. Although much of the dark web's information is Open-Source Data (OSD), it can also be used as Open-Source Intelligence (OSINT), despite efforts to conceal it through anonymous networks and encryption. Because of this, the dark web has become increasingly important in fighting financial crime and other illicit activities. As criminals become more technically sophisticated, they are increasingly shifting their activities to the dark web. Although investigative procedures and technological capabilities enhance the challenge, access to the "right" tools to be effective is still challenging. The dark web is often associated with illicit activities, including the sale of illegal drugs, weapons, and stolen data, as well as the trade in illegal pornography and the facilitation of cybercrime and human trafficking. As such, dark web monitoring can be a valuable tool for organizations and law enforcement agencies looking to gather intelligence, identify potential threats, and support ongoing investigations. Furthermore, the rise of new users, including illicit goods sellers, to the dark web due to recent scrutiny of surface web activities has made this issue even more pressing. The dark web has gained widespread notoriety, and criminals are becoming more technically sophisticated, which makes it increasingly challenging to combat the illegal activities conducted within this hidden network.

This research paper aims to highlight the importance of dark web monitoring for open-source intelligence (OSINT) and investigations. It will show an overview of the most prevalent darknets on the dark web, the technologies behind them, their size and popularity, and the kind of information they contain using OSINT that enhances making deep

investigations. The paper will explore ways dark web monitoring can be used for OSINT gathering and investigations, and how advanced techniques such as AI and machine learning can enable analysts to identify and mitigate cyber threats more efficiently and effectively.

2. SELECTION OF PAPERS BY PRISMA

SLR, or systematic literature review, is a methodology used to select a minimal set of studies from a wide array of stud- ies. This is a significant reason for its use in this paper. In the first step, the Searched by Saudi Digital Library and google scholar databases using the querying combination of the fol- lowing keywords: (Dark web or Deep web) AND crime AND (Monitoring OR OSINT OR Investigations). The lit- erature is confined to studies published between 2018 and 2022 in English. Google Scholar revealed 2300 papers that speak specifically about dark web crimes and how they can be used for monitoring OSINT investigations. These 2300 search papers were registered, removing 1200 duplicates be- fore screening and 700 papers for other reasons. Also, 1000 papers we revealed in the Saudi Digital library. 600 pa- pers have been excluded after screening the title and ab- stract because of unspecific goals. 200 and 350 papers were assessed for eligibility from the Google Scholar and Saudi Digital Library databases, respectively. Finally, after review- ing and studying these papers, we selected 15 papers from the Google Scholar database and 5 from the Saudi Digital Library. This selection process for papers by PRISMA is shown in Figure 1.

3. LITERATURE REVIEW

The literature review provides an overview of the current state of knowledge regarding the use of the dark web for criminal activities and the importance of dark web monitor- ing for open-source intelligence (OSINT) and investigations. The reviewed studies focus on various aspects of the dark web, including the methods used by criminals to carry out cybercrime activities, the types of cyberattacks and activi- ties that originate from darknets and black-market sources, the use of OSINT techniques in investigations of child abuse material (CAM) on the dark web, and the potential of OSINT to prevent fraud.

The literature review also examines the challenges and lim- itations associated with investigating and detecting darknet and black market activities, the ethical and legal consider- ations of using OSINT for password cracking and investi- gating CAM on the dark web, and the need for collabora- tion and information sharing among investigators and other stakeholders in the field.

Overall, the literature review provides a foundation for the research in this paper, which aims to highlight the impor- tance of dark web monitoring for OSINT and investigations, and explore advanced techniques such as AI and machine learning that can enable analysts to identify and mitigate cy- ber threats more efficiently and effectively.

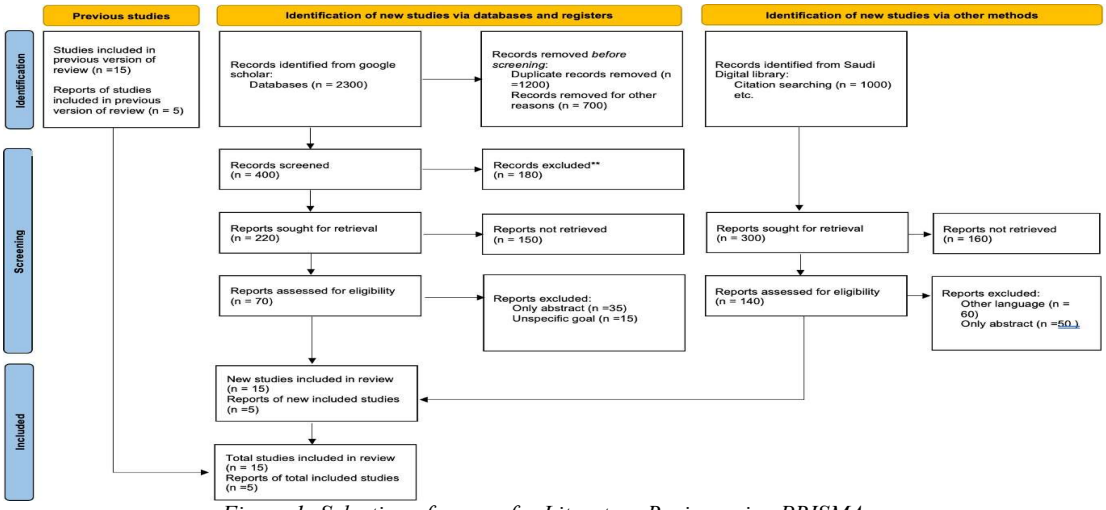

Figure 1: Selection of papers for Literature Review using PRISMA.

Several research studies have been examined and summa- rized below in a brief description of these studies. The Dark Web allows users to hide their identity when surfing or trans- ferring data. The Dark Web is a perfect setting for exchang- ing possibly illicit information, commodities, and services. Law enforcement agencies (LEAs) are interested in dark web Open Source Intelligence (OSINT). This article looks into the numerous OSINT automation tools that criminals might use on the Dark Web Horan, C. et al [1].

The study aims to explore the current landscape of cyber- crime investigations, the challenges faced by investigators, and potential future research directions in this field. The study focused on identifying the different types of cyber- crime and the methods used by criminals to carry out these activities. Additionally, the study examined the current state of cybercrime investigation practices, including the use of digital forensics, incident response, and cyber intelligence. discussed the challenges faced by investigators, such as lack of resources, legal and technical limitations, and the need for cross-disciplinary collaboration. The study suggested future research directions, such as the development of new tech- nologies and techniques to improve cybercrime investiga- tions and the need for more collaboration and information sharing among investigators and other stakeholders in the field. More than only the investigators are affected by cy- ber investigations. To be most successful, tools employed in digital forensics and open-source intelligence investigations must be coupled. The most effective and least likely to cause data destruction are logical extraction and hex dumps. Natu- ral language processing has more applications and uses than the other options combined [2].

Many sorts of drug offences have previously been recog- nized, but offender groupings are widespread. According to a new Europol report, a successful liquidation of Dark Mar- ket, one of the largest illicit marketplaces, occurred, necessi- tating the collaboration of multiple European Union Member States as well as several non-European Union nations. The Dark Web (a secret network) has grown in popularity over the platforms that link to the Dark Web [3].

The Silk Road's popularity has fueled the establishment of several dark web markets. This exponential expansion has offered new channels for criminal companies to market un- lawful goods. Traditional Web scraping technologies and investigation techniques have been ineffective at identifying market players [4].

It is possible to locate particular information that has some expertise or gives an advantage by using OSINT. As a result, the goal of this study is to conduct a comprehensive literature review on OSINT in order to examine the use of OSINT with AI [5].

Kanta, A. et al [6] study aimed to explore how Open-source intelligence (OSINT) can be used to improve the efficiency and effectiveness of password cracking. The survey may have investigated various methods and tools that can be used to gather information about potential targets and their pass- words, such as social media scraping, email harvesting, and domain surveys, as well as the ethical and legal implica- tions of using OSINT for password cracking. The survey may have also highlighted the benefits of using OSINT for password cracking, including gathering more targeted infor- mation, increasing the chances of success, and reducing the number of potential passwords that need to be tested.

Akintaro, Mojolaoluwa, et al [7] The survey aims to explore the threat and impact of darknet and black market activities on cybersecurity. The study may have focused on identi- fying the most common types of cyberattacks and activities that originate from darknets and black-market sources, such as hacking, malware, phishing, and cyberfraud. Addition- ally, the survey examined the methods and techniques used by cybercriminals to carry out these activities, such as the use of Tor networks and encryption, as well as the measures that organizations can take to protect themselves from these threats. The survey also discussed the challenges and limita- tions of investigating and detecting darknet and black market activities.

Rajama ki, J [8] The study aims to explore the use of open- source intelligence (OSINT) techniques in investigations of child abuse material (CAM) on the dark web. The study fo- cused on identifying the different types of CAM found on the dark web and the methods used by criminals to distribute and

access this material. Additionally, the study examined the use of OSINT tools and techniques such as dark web scrap- ing, metadata analysis, and data visualization to gather and analyse information on CAM distribution networks. Also discussed are the challenges and limitations of using OSINT for investigating CAM on the dark web, such as the need for specialized knowledge and skills and the ethical and legal considerations

of conducting OSINT on the dark web.
Chalicheemala, Det al [9] The study aims to explore the con- cept of open-source intelligence (OSINT) and its potential to prevent fraud. The study covered the definition of OS- INT, the different types of information and sources used in OSINT, and the methods and techniques used to collect, an- alyze, and disseminate OSINT information. Additionally, it examined the use of OSINT in fraud prevention, such as well as the ability to identify and track fraudsters, uncover fraud- ulent schemes, and support investigations. Also discussed are the challenges and limitations of using OSINT for fraud prevention, such as the need for specialized knowledge and skills and the ethical and legal considerations of conducting OSINT. and provided insights and recommendations for or- ganizations to effectively use OSINT in preventing fraud.

4. WHAT IS DARK WEB?

The dark web is a part of the internet that is not indexed by search engines and can only be accessed using special- ized software, such as the Tor browser. It is often associated with illegal activities, such as the sale of illegal goods and services, but it is also used for legitimate purposes, such as anonymous communication and the sharing of sensitive in- formation [10].
Dark Web monitoring can be used for a variety of purposes, including open-source intelligence (OSINT) gathering and investigations. Here are some examples of how dark web monitoring can be used in these contexts:
OSINT gathering: By monitoring the dark web, investiga- tors can gather valuable intelligence about individuals or or- ganizations. This can include information about their activities, connections, and intentions.
Investigating cybercrimes: The dark web is often used as a platform for cybercriminals to buy and sell stolen data, mal- ware, and other illicit goods and services. By monitoring the dark web, investigators can gather evidence and identify suspects in cases involving cybercrime.
Identifying potential threats: By monitoring the dark web, investigators can identify potential threats to an organization or individual. This can include the sale of sensitive informa- tion or the planning of attacks.
Tracking the activities of suspects: By monitoring the dark web, investigators can track the activities of suspects and gather evidence that can be used in an investigation. DaTheebs are the result of a US Naval Research Laboratory- funded project in the 1990s that attempted to protect intelli- gence communications using a network of relays known as the Onion Routing (Tor) Project to route traffic. As a result, Tor has attracted the support of numerous organisations and institutions, including Human Rights Watch, Facebook, and Google The dark web is certainly a place where you can find some espionage activity, even if it has little to do with illicit activity [11].

- Prior to the 2015 Paris terrorist attacks, ISIS spread pro- paganda on onion forums, one of the 50,000 terrorist networks communicating on the dark
- A total of 1% of dark web addresses are dedicated to fi- nancial crime. In 2020, 133,927 C-level executive cre- dentials were found on dark web marketplaces. Typ- ically, personal information and sensitive information, such as social security numbers and credit card num- bers, can be sold for as little as $1.
- Dark web markets are dominated by drugs, with 48% of listings being related to
- Weapons: Illegal weapons, including firearms and ex- plosives, are readily available for purchase on the dark web.
- Child pornography: disturbing and illegal content, in- cluding child pornography, is also available on the

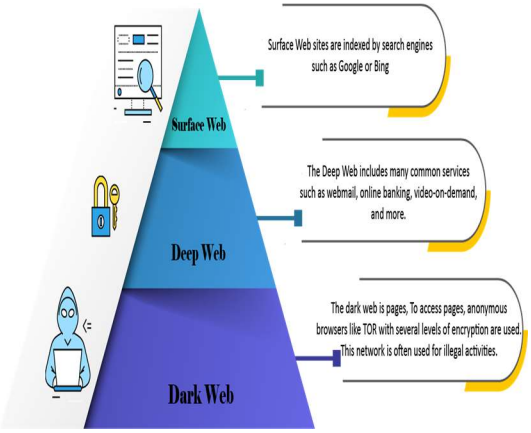

Figure 2: Layers Of The Web

5. THE MOST FAMOUS CRIMES OF THE DARK WEB

Silk Road was a dark web marketplace that was launched in 2011 and was used to facilitate the sale of illegal drugs, stolen data, and other illicit

goods and services. The site op- erated using the TOR network and accepted payments in the form of Bitcoin, making it difficult to trace transactions and identify users. The operator of Silk Road, Ross Ulbricht, was arrested in 2013 and later convicted of money laundering, computer hacking, and conspiracy to traffic narcotics (United States Department of Justice, 2015) [12].

In addition to Ulbricht, several other individuals were also arrested and charged in connection with their involvement in Silk Road. These individuals included Andrew Michael Jones, who was convicted of conspiracy to distribute con- trolled substances and money laundering (United States De- partment of Justice, 2015), and Peter Philip Nash, who was convicted of conspiracy to commit computer hacking and conspiracy to traffic narcotics (United States Department of Justice, 2015).

Overall, Silk Road was a significant criminal enterprise that facilitated the sale of illegal drugs and other illicit goods and services on the dark web. The arrest and conviction of its operator and other individuals associated with the site helped to disrupt this illegal activity and send a message that such crimes will not be tolerated.

One of the most important criminals on the dark web is Shan- non McCoole, a former child protection worker in South

Australia who was convicted of multiple counts of sexual abuse against children in his care. McCoole was arrested in 2014 as part of a global investigation into the distribution of child pornography on the dark web. He was subsequently convicted and sentenced to 35 years in prison, with a non- parole period of 28 years (Australian Federal Police, 2015). According to media reports, McCoole used the pseudonym "Skee" on the dark web and was a member of an interna- tional child abuse network known as "The Love Zone." He was responsible for producing and distributing child pornog- raphy and facilitating the sexual abuse of children by other members of the network [13].

The case of Shannon McCoole highlights the disturbing prevalence of child abuse and exploitation on the dark web and the importance of law enforcement efforts to disrupt and dismantle such networks.

In 2017, the WannaCry ransomware attack affected hundreds of thousands of computers in more than 150 countries. The attackers used a hacking tool stolen from the US National Security Agency and offered it for sale on the dark web. The WannaCry attack was a reminder of the threat posed by ma- licious actors on the dark web, who can use stolen tools and techniques to launch devastating cyberattacks. WannaCry was particularly notable because of the scale and speed of the attack, which affected hundreds of thousands of comput- ers in more than 150 countries in just a few hours. The attack was able to spread quickly due to a vulnerability [14].

In Microsoft Windows that the attackers were able to exploit. The WannaCry attack was attributed to a hacking group that is believed to be based in North Korea. The group used a hacking tool known as "EternalBlue," which was stolen from the US National Security Agency and was later offered for sale on the dark web. The WannaCry attack was a reminder of the dangers posed by the dark web, where stolen tools and techniques can be easily obtained and used by malicious actors to launch devastating cyberattacks. In the aftermath of the WannaCry attack, Microsoft issued a patch to fix the vulnerability in Windows that was exploited by the attackers. The company also called on other technology companies to work together to combat the threat posed by ransomware and

other forms of malware. The WannaCry attack is a prime example of the importance of keeping software up-to-date and implementing robust cybersecurity measures to protect against attacks [15].

AlphaBay was a dark web marketplace that was active from 2014 to 2017. It was one of the largest dark web mar- ketplaces and was known for being a hub for selling il- legal drugs and other illicit goods and services, such as firearms, counterfeit goods, and stolen data. AlphaBay used the anonymous network Tor and cryptocurrency, such as Bit- coin, to maintain the anonymity of its users. This anonymity made it difficult for law enforcement agencies to track and identify those involved in illegal activities on the market- place. In July 2017, AlphaBay was shut down due to a joint law enforcement operation by the FBI, DEA, and Europol. The process resulted in the arrest of the creator and operator of the marketplace, Alexandre Cazes, who was found dead in his cell in Thailand while awaiting extradition to the United States. The shutdown of AlphaBay was significant as it dis- rupted a major hub for illegal activities on the dark web and sent a strong message to other

dark web marketplaces and their users that law enforcement agencies are actively moni- toring and targeting illegal activities on the dark web [16]. Operation Pacifier: In 2015, the FBI launched Operation Pacifier, an operation aimed at disrupting and shutting down the Playpen child exploitation website on the dark web. The site was used for the distribution and sale of child exploita- tion material, including child pornography and videos of child abuse. The FBI was able to gain control of the site and use it to track and identify those who were using it to access and distribute child exploitation material. As a result of the operation, hundreds of individuals were arrested and charged with crimes related to child exploitation and abuse. The FBI used a network investigative technique (NIT) to gather infor- mation about the users of the Playpen site. The NIT allowed the FBI to obtain the IP addresses and other identifying infor- mation of those who were accessing the site, which was used to track and arrest the individuals involved. However, the use of NITs and other hacking techniques by law enforcement has raised questions about privacy and the potential abuse of power. Some have criticized the operation as a violation of privacy and civil liberties and have called for increased oversight and accountability of law enforcement activities on the dark web. Despite these concerns, Operation Pacifier is widely seen as a significant victory in the fight against child exploitation on the dark web. The operation disrupted a sig- nificant source of child exploitation material and led to the arrest of hundreds of individuals involved in these crimes. It also serves as a warning to those who would use the dark web for illegal activities and highlights the continued efforts of law enforcement to combat crime on the platform [17].

The Hansa Market bust: In 2017, Dutch law enforcement agencies conducted a coordinated operation aimed at shut- ting down the Hansa Market, one of the largest online black markets on the dark web. The operation involved taking con- trol of the site and using it to monitor and gather information about its users. The Dutch police were able to identify and arrest the individuals behind the site, including the admin- istrators and those involved in illegal activities on the plat- form. They were able to gather significant amounts of evi- dence about the transactions and activities that were taking place on the site, which was used to prosecute those involved. Additionally, the Hansa Market bust served as a warning to those who would use the dark web for illegal activities, and it sent a message to the wider public about the dangers as- sociated with the platform. It also raised questions about the balance between privacy and security and the use of in- vestigative techniques by law enforcement. This operation demonstrated the global reach of law enforcement and the cooperation between international agencies in their efforts to tackle crime on the dark web. It also showed the potential for law enforcement to effectively disrupt and shut down illegal sites on the platform, reducing the harm caused by criminal activities. However, the dark web continues to pose a signif- icant challenge for law enforcement, and it remains a place where individuals can engage in illegal activities with rela- tive anonymity. As technology continues to evolve, the need for ongoing efforts to combat crime on the dark web remains important [18].

6. WHAT IS DARK WEB MONITORING?

Dark web monitoring is the process of monitoring and track- ing activities that take place on the dark web, a part of the internet that is not indexed by search engines and can only be accessed using specialized software such as the Tor browser. The dark web is a place where people can engage in illegal activities and access illegal content, including illegal drug trade, human trafficking, and the sale of stolen credit card information.

Dark web monitoring can be performed by individuals or or- ganizations as a means of protecting their own interests and staying aware of potential threats. This can involve using specialized tools to scan the dark web for certain keywords or monitoring specific websites or forums that are known to be associated with illegal activity.

Some businesses and organizations also use dark web moni- toring as a way to detect and prevent data breaches by moni- toring the dark web for the sale of their own or their clients' sensitive data.

The 21st century has brought us new tools for forensic inves- tigations that are powered by artificial intelligence, fighting fire with fire on the dark web. In order to monitor the dark web, law enforcement agencies can use AI web intelligence software to use dark web investigation tools. As a result, they can identify threat actors and malicious activity more effec- tively, solve cases faster, stay ahead of threats, and enhance existing and offline investigations.

It has been possible to develop new techniques to break through the barriers that often prevent dark

web crawlers from accessing hotspots for criminal activity, such as dark web forums.

6.1 Who Benefits From The Monitoring Of The Dark Web?

There are several groups that can benefit from the monitoring of the dark web:

- Individuals: Individuals who are concerned about their online security and privacy can use dark web monitor- ing to stay informed about any potential threats and take steps to protect themselves.
- Businesses: Businesses can use dark web monitoring to protect their sensitive data, such as customer informa- tion and intellectual property.
- By monitoring the dark web for the sale of their data, businesses can detect and prevent data breaches.
- Governments: Governments can use dark web moni- toring to track and investigate illegal activities such as cybercrime, human trafficking, and the sale of illegal drugs.
- Law enforcement agencies: Law enforcement agencies can use dark web monitoring to gather intelligence and evidence for criminal investigations.
- Cyber security professionals: Cyber security profes- sionals can use dark web monitoring to stay informed about the latest threats and techniques used by hackers and cybercriminals. This can help them better protect their organizations and clients.

As a means of combating cybercrime and terrorism, major governmental authorities are using dark web monitoring to prevent it from happening. As a form of neighbourhood watch, agencies such as the FBI, Drug Enforcement Admin- istration, and Homeland Security use AI crime prediction software and dark web crawlers to keep an eye on suspicious activities that might be part of a bigger investigation.

As a detective or investigator, you often have to transform raw data into actionable information in order to solve a prob- lem. Cobwebs is a web intelligence platform that takes data from dark web sources such as blogs, social networks, im- ported files, and deep web data and analyzes it using big data to reveal crucial connections between the locations, cyber footprints, and affiliations of threat actors. As part of the in- telligence insights, the wide range of crawling grounds has been included. By doing so, you are able to convert impor- tant words and phrases into valuable leads in the long run.

6.2 How Does Dark Web Monitoring Work?

Dark web monitoring typically involves the use of special- ized tools and software to scan the dark web for certain keywords or to monitor specific websites or forums that are known to be associated with illegal activity. These tools may be provided by cyber security companies or may be devel- oped in-house by businesses or organizations [19].

To access the dark web, users typically need to use special- ized software such as the Tor browser, which encrypts inter- net traffic and routes it through a series of servers around the world to obscure the user's identity. This makes it difficult for law enforcement agencies and others to track the activi- ties of users on the dark web.

Dark web monitoring tools may use a variety of techniques to scan the dark web, including:

- Keyword monitoring: This involves using software to scan the dark web for specific keywords that may be associated with illegal activities or the sale of sensitive data.
- Website monitoring: This involves monitoring specific websites or forums on the dark web that are known to be associated with illegal activities.
- Link analysis: This involves analyzing the links be- tween different websites and forums on the dark web to identify patterns and connections that may be associ- ated with illegal activity.
- Intelligence gathering: This involves collecting and an- alyzing information about activities on the dark web to identify trends and patterns that may be indicative of illegal activity.

7. THE DARK WEB IN OSINT IN- VESTIGATIONS

The dark web can be a useful source of information for Open Source Intelligence (OSINT) investigations, which involve collecting and analyzing publicly available information from a variety of sources. However, it is important to note that the

dark web is a place where illegal activities often take place, and accessing the dark web and participating in any illegal activities is illegal in most countries. Therefore, it is impor- tant to only use the dark web for legitimate purposes and to seek legal guidance if you have any concerns about the le- gality of your actions.

That being said, the dark web can be a valuable source of information for OSINT investigations because it can provide access to information that is not readily available on the open web. For example, the dark web may contain forums or web- sites that are only accessible to a specific group of people, such as members of a criminal organization or individuals who have purchased illegal goods or services.

To access the dark web, investigators typically need to use specialized software such as the Tor browser, which encrypts internet traffic and routes it through a series of servers around the world to obscure the user's identity. This makes it dif- ficult for law enforcement agencies and others to track the activities of users on the dark web.

It is important for investigators to be cautious when using the dark web for OSINT investigations, as the information obtained may not always be reliable or accurate. It is also important to ensure that all information collected from the dark web is obtained legally and ethically.

7.1 Dark Web Monitoring With OSINT

Although it is technically possible to create your own dark web monitoring program, it is unrealistic. A high level of computational power and systematization will be required to continuously scan the dark web for platforms where personal information is sold or traded. Making the right business plan and finding the right solutions based on the problem is one of the challenges of the job.The purpose of this article is to provide you with a simple methodology comprised of a few steps and a set of tools that allow you to automate these steps. The steps are mainly as follows:

- How to get onion links over TOR
- How to search these links
- How to collect the data through these connections
- How to process this data

7.2 How the Dark Web Can Be Used in OS- INT Investigations

As OSINT investigators begin to venture into the dark web To get a better understanding of illicit networks and criminal activity, the dark web has become a very valuable source of insight into these activities [20]. Let's examine some of the opportunities the dark web can provide:

- **Monitoring Illicit Activities** The dark web's forums, marketplaces, and messaging services can be easily ac- cessed, allowing you to monitor users and discussions quickly, as well as monitor illicit activities. As a re- sult, detectives can use dark web sites to gain a deeper understanding of contemporary trends in drug dealing, financial crime, firearms sales, even human trafficking and wildlife [21]
- **Evaluating Existing Leads** In order to evaluate exist- ing leads, you can use the dark web whistleblowing re- sources such as Global Leaks, Independent Media Cen- ter, as well as other services provided by the Ameri- can Whistleblowing Press to evaluate leads that already exist. It is also possible to corroborate or disprove in- formation that is found on the surface web through this method [22].
- **Combating Insider Threats** When a company's data is breached, leaked, or hacked, dark web marketplaces and forums can provide evidence that the data has been sold to the dark web and by whom as a result of in- sider threats. Additionally, insider threats may reveal information about themselves that is either identifiable or incriminating in nature [23].
- **Identifying Individuals** Despite the implied safety pro- vided by the dark web, poor user habits can lead to un- intended self-identification on the dark web, despite the implied safety of the dark web. As an example, users of dark web forums might use the same usernames they use on social networks, or their language, terminology, or profile picture may appear to match that of surface
web users [24].

7.3 Dark Web Challenges in OSINT Investi- gations

In spite of the potential benefits of utilizing thedark web for threat intelligence and investigation, it is critical that we first understand the challenges that dark web searches and data mining present to investigators in the area of threat intelli- gence and investigation [25]:

- Despite not having a surface web search engine such as Google indexing the dark web, special dark web search engines are available to explore the dark web, although these search engines are typically slow and cumbersome. It is common for dark web addresses to be changed in order to make it hard to trace them.

- This is an important point to emphasize because browser fingerprinting is a tracking method that sub- verts onion routing security. Although it may be nearly impossible to track users directly through their data traf- fic, browser fingerprinting uses unique properties of the browser and machine to identify users.
- With Tor, you are protected from fingerprinting by blocking scripts, using the same default fallback fonts on all browsers, and blocking WebGL and the Canvas API, so it is difficult to differentiate between browsers, thus making it difficult to distinguish between them. In spite of this, the Tor Project admits that it may even- tually be possible to identify users based on their Tor browser fingerprint.
- Keeping humans out of the loop: Researchers are sus- ceptible to human error in the same way that dark web users are susceptible to revealing their own OSINT in- vestigators will be able to use their existing skills when searching the dark web, but it is important to be care- ful not to leave behind any evidence when they search. As a result, researchers may become weary and more prone to errors when performing exhaustive OSINT op- erations.
- An individual may be exposed to illegal or potentiallytraumatic material through the dark web if they are ex- posed to Many of the pages on the dark web are in- tentionally uncensored or unmoderated, allowing them to spread illegal and potentially traumatic material. It presents a legal and ethical dilemma for researchers: they must develop strategies that ensure that certain types of content are moderated or triaged before they are able to access them at a distance.

8. SOLUTION

1. Developing and implementing advanced technologies and techniques such as AI and machine learning can significantly enhance dark web monitoring and analysis for OSINT and investigations. Some potential ways in which these technolo- gies can be utilized include:

Automated identification of dark web content: AI and machine learning algorithms can be trained to automatically identify and extract relevant information from dark web con- tent, such as forums, marketplaces, and social media chan- nels. This can help analysts to quickly and efficiently iden- tify potential threats and gather intelligence.

Sentiment analysis: AI and machine learning can be used to analyze the sentiment of dark web content, which can pro- vide valuable insights into the activities and motivations of individuals and groups operating on the dark web.

Network analysis: Advanced techniques such as machine learning can be used to identify patterns and connections among individuals and groups on the dark web. This can help investigators to build a comprehensive picture ofcrimi- nal networks and identify key actors and activities.

Image recognition: AI and machine learning can be trained to recognize specific images and objects on the dark web, such as images of illegal drugs or weapons. This can help to quickly identify illicit activities and facilitate investigations. **Prediction and forecasting:** Machine learning algorithms can be used to predict future trends and patterns on the dark web, such as changes in the types of activities or the emer- gence of new criminal networks. This can help law enforcement agencies to proactively identify and mitigate potential threats.

2. Encouraging collaboration and information sharing among investigators and other stakeholders in the field is essential to enhancing the effectiveness of dark web moni- toring and investigation practices. Some potential ways to achieve this include:

Sharing information and intelligence: Law enforcement agencies and other stakeholders can share information and intelligence about dark web activities and trends to enhance their understanding of the threat landscape and facilitate in- vestigations.

Developing collaborative partnerships: Partnerships can be developed between law enforcement agencies, academic institutions, private companies, and other stakeholders to fa- cilitate the sharing of knowledge and expertise, and promote a more coordinated approach to dark web monitoring and in- vestigation.

Building trust and relationships: Building trust and re- lationships among stakeholders is essential to facilitate in- formation sharing and collaboration. This can be achieved through regular communication, joint training, and the de- velopment of shared objectives and goals.

Standardizing practices and protocols: Standardizing dark web monitoring and investigation practices and pro- tocols can help to ensure consistency and interoperability among stakeholders, and facilitate the exchange

of informa- tion and intelligence.

Encouraging innovation and experimentation: Encourag- ing innovation and experimentation among stakeholders can help to drive the development of new tools and techniques for dark web monitoring and investigation, and promote a more effective and efficient approach to combating cybercrime and other illicit activities.

3. Leveraging the data obtained through dark web monitor- ing and analysis can help identify and mitigate cyber threats more efficiently and effectively. Some ways in which this can be achieved include:

Identifying key actors and activities: The data obtained through dark web monitoring and analysis can help identify

key actors and activities associated with cyber threats, such as malware distribution, phishing attacks, and hacking.

Analyzing attack patterns: By analyzing the data obtained through dark web monitoring and analysis, investigators can identify attack patterns and tactics used by cybercriminals, which can inform the development of more effective defense strategies.

Developing threat intelligence: The data obtained through dark web monitoring and analysis can be used to develop threat intelligence, which can inform decision-making and help organizations prioritize their cybersecurity efforts.

Enhancing situational awareness: By monitoring the dark web, organizations can gain a better understanding of the current threat landscape and enhance their situational aware- ness, enabling them to detect and respond to threats more quickly.

Supporting investigations: The data obtained through dark web monitoring and analysis can provide valuable evidence to support investigations into cyber threats, such as identi- fying the source of an attack or tracking the activities of a particular cybercriminal.

4. Increasing awareness and education on the risks and dan- gers associated with using the dark web for criminal activ- ities is crucial to discourage individuals from engaging in illicit behavior. Some ways in which this can be achieved include:

Educating the public: Governments, law enforcement agencies, and other stakeholders can launch public aware- ness campaigns to educate the public on the risks and dan- gers associated with using the dark web for criminal activi- ties.

Highlighting the consequences: Education efforts should also highlight the legal consequences of engaging in illicit behavior on the dark web, such as the risk of arrest, impris- onment, and financial penalties.

Collaborating with educational institutions: Collabora- tion with educational institutions can help to raise awareness of the dangers of the dark web among young people, who may be particularly vulnerable to engaging in illicit behavior online.

Offering alternative solutions: Providing alternative solu- tions to criminal activities, such as legal avenues for purchas- ing goods and services, can help to discourage individuals from turning to the dark web for such activities.

Providing support for victims: Education efforts should also highlight the harm caused by criminal activities on the dark web, and provide support and resources for victims of such crimes.

5. Developing and implementing policy and regulatory frameworks is crucial to addressing the challenges and lim- itations associated with investigating and detecting darknet and black market activities. Such frameworks can help en- sure that investigations are conducted ethically and legally, while also promoting greater effectiveness in combating cy- bercrime and other illicit activities. Some ways in which this can be achieved include:

Establishing guidelines and best practices: Policy and reg- ulatory frameworks can establish guidelines and best prac- tices for investigating and detecting darknet and black market activities, which can help to ensure consistency and ethical conduct among investigators and other stakeholders.

Ensuring compliance with laws and regulations: Policy and regulatory frameworks can help ensure compliance with existing laws and regulations related to darknet and black market activities, as well as promote the development of new legal and regulatory measures to address emerging threats.

Promoting collaboration and information sharing: Policy and regulatory frameworks can promote collaboration and information sharing among investigators, law enforcement agencies, and other stakeholders, which can enhance the ef- fectiveness of dark web monitoring and investigation prac- tices.

Balancing privacy and security concerns: Policy and regu- latory frameworks can help balance privacy and security con- cerns, ensuring

that investigations are conducted in a manner that respects individual rights and freedoms, while also pro- moting public safety and security.

Enhancing accountability and oversight: Policy and regu- latory frameworks can enhance accountability and oversight of investigations and detection activities, ensuring that they
are conducted in an ethical and transparent manner.

9. CONCLUSION

The rise in the severity and complexity of cyber threats from various parts of the internet has led organizations to explore new solutions to mitigate the risks. Open Source Intelligence (OSINT) has emerged as a critical solution that can be used to obtain information from dark web sites that are commonly used by cybercriminals to share information about successful attacks, vulnerabilities, and the latest tools and techniques. The dark web is a hidden network of websites that can only be accessed using specialized software and are not indexed by search engines.

To effectively use the dark web for OSINT, it is essential to employ a dark web monitoring tool that can collect informa- tion from the dark web and process it to identify useful open- source intelligence. The gathered data can provide valuable contextual information to analysts about the current state of the cyber threat landscape. The analysis of this information can help organizations take proactive steps to reduce the risks of cyber-attacks.

In the future, OSINT may increasingly use artificial intelli- gence, machine learning, language processing, and ontology approaches to respond properly and proactively to the con- stantly changing cyber environment. These advanced tech- niques can enable analysts to identify and mitigate cyber threats more efficiently and effectively. While it may not be possible to eradicate all threats from the dark web entirely, proactive countermeasures can significantly reduce the se- vere effects of the threats lurking within this hidden network. The use of dark web monitoring tools and advanced tech- niques such as AI and machine learning can help organiza- tions gather valuable intelligence from the dark web and re- spond effectively to the growing threat of cyber-attacks. By maintaining a high level of precision, potency, and efficiency in their countermeasures, analysts can protect organizations from the damaging effects of cyber threats originating from the dark web. In conclusion, while the dark web may pose
a significant risk to organizations, the use of OSINT and ad- vanced technology can help mitigate these risks and enable organizations to stay ahead of cybercriminals.

FUNDING: This work was funded by King Faisal Univer- sity, Saudi Arabia [Project No. GRANT3,344].

ACKNOWLEDGMENTS: This work was made possible in part by a grant from the university, which allowed us to conduct the research and collect the necessary data. This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Grad- uate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT3,344].

CONFLICTS OF INTEREST: All authors declare no con- flict of interest.

REFERENCES

[1] Davies, G.: Shining a light on policing of the dark web: An analysis of uk investigatory powers. The Journal of Criminal Law **84**(5), 407–426 (2020)

[2] Horan, C., Saiedian, H.: Cyber crime investigation: Landscape, challenges, and future research directions. Journal of Cybersecurity and Privacy **1**(4), 580–596 (2021).https://www.mdpi.com/2 624-800X/1/4/29

[3] Clough, J.: Principles of Cybercrime. Cambridge Uni- versity Press, ??? (2015)

[4] Hayes, D.R., Cappa, F., Cardon, J.: A framework for more effective dark web marketplace investigations. In- formation **9**(8), 186 (2018)

[5] Kalpakis, G., Tsikrika, T., Cunningham, N., Iliou, C., Vrochidis, S., Middleton, J., Kompatsiaris, I.: OSINT and the Dark Web, pp. 111–132. Cham: Springer Inter- national Publishing, ??? (2016)

[6] Kanta, A., Coisel, I., Scanlon, M.: A survey exploring open source intelligence for smarter password crack- ing. Forensic Science International: Digital Investiga- tion **35**, 301075 (2020)

[7] Akintaro, M., Pare, T., Dissanayaka, A.M.: Darknet and black market activities against the cybersecurity: A survey. In: The Midwest

Instruction and Comput- ing Symposium.(MICS), North Dakota State Univer- sity, Fargo, ND (2019)
[8] Rajamäki, J., Lahti, I., Parviainen, J.: Osint on the dark web: Child abuse material investigations. Information & Security: An International Journal **53**, 21–32 (2022)
[9] Chalicheemala, D., Chalicheemala, D.: What is open- source intelligence and how it can prevent frauds. SSRN Electronic Journal (2022)
[10] BBC News: Dark web: What it is and how to access it.https://www.bbc.com/news/technology-53463026(2022)
[11] Ragan, S: How law enforcement tracks suspects in the dark web. Security Boulevard (2021). https://securityboulevard.com/2021/02/how-law- enforcement-tracks-suspects-in-the-dark-web/
[12] United States Department of Justice: Ross Ulbricht, AKA "Dread Pirate Roberts," Sentenced To Life In Prison.https://www.justice.gov/usao-sdny/pr/ross- ulbricht-aka-dread-pirate-roberts-sentenced-life-prison (2015)
[13] Australian Federal Police: Former child protection worker sentenced to 35 years' jail for child sex crimes.https://www.afp.gov.au/news-media/media- releases/former-child-protection-worker-sentenced-35- years-jail-child-sex-crimes(2015)
[14] BBC News: What is WannaCry ransomware and why is it attacking global computers? https://www.bbc.com/news/technology-39901382 (2017)
[15] Greenberg, A: The WannaCry ransomware hack- ers made some real amateur mistakes. Wired. https://www.wired.com/story/wannacry-ransomware- hackers-mistakes/(2017)
[16] United States Department of Justice: Alleged Al- phaBay founder, Alexandre Cazes, found dead in Thai jail cell.https://www.justice.gov/opa/pr/alleged-alphabay-founder-alexandre-cazes-found-dead-thai- jail-cell(2017)
[17] United States Department of Justice: "Playpen" Creator Sentenced to 30 Years in Prison for Oper- ating Largest Child Sexual Exploitation Site Ever Prosecuted.https://www.justice.gov/opa/pr/playpen- creator-sentenced-30-years-prison-operating-largest- child-sexual-exploitation-site(2016)
[18] van Ham M & van Ham R: The Hansa Market bust: The dark web's downfall or a momentary blip? (2019) [19]What Is Dark Web Monitoring?: How does it work? — aura. Global Crime (2022).www.aura.com/learn/what-is-dark-w eb-monitoring, Accessed 30 Dec [20]Clarke S: Osint investigations: The challenge of dark web and data mining. Blackdot Solutions Videris (2022).https://ww w.blackdotsolutions.com/blog/dark- web-dat a-searches-and-mining
[21] Pastor-Galindo, J., Nespoli, P., Mármol, F.G., Pérez, G.M.: The not yet exploited goldmine of osint: Oppor- tunities, open challenges and future trends. IEEE Ac- cess **8**, 10282–10304 (2020)
[22] Liu, Y., Lin, F., Ahmad-Post, Z., Ebrahimi, M., Zhang, N., Hu, J., Xin, J., Li, W., Chen, H.: Identifying, collecting, and monitoring per- sonally identifiable information: From the dark web to the surface web. In: Proceedings - 2020 IEEE International Conference on Intelligence and Security Informatics, ISI 2020, pp. 1–6 (2020). http://dx.doi.org/10.1109/ISI49825.2020.9280540
[23] Borges Esteban: What is OSINT? How can I make use of it? Security trails.https://security trails.com/blog/what-is-osint-how-can-i-mak e-use-of- it(2021)
[24] Yong-Woon Hwang, Im-Yeong Lee, Hwankuk Kim, Hyejung Lee, Donghyun Kim: Current status and security trend of osint. Wireless Com- munications and Mobile Computing, 14 (2022). http://dx.doi.org/10.1155/2022/1290129
[25] P, P.: Dark Web users of a child porn website tracked after visiting file sharing site. Security Affairs. https://securityaffairs. co/wordpress/ 59632/cyber- crime/dark-web-c hildporn.html(2017)