iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52985

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

A Comprehensive Study of Dark Net

Varun Suresh Kallen[1], K.V. Ravi Kumar[2*]
[1]*Amity Institute of Forensic Sciences, Amity University, Sector 125, Noida, Uttar Pradesh, 201301*
[2]*Associate Professor, Amity Institute of Forensic Sciences, Amity University, Noida, Uttar Pradesh, India*

***Abstract:** This review explores the utilization of the dark web, which is one of the three parts of the internet, along with the surface web and the deep web. The dark web is infamous for being a hidden space where illegal activities, including cybercrime, take place. This paper delves into the history and nature of these spaces, as well as the attention they receive from the media. Additionally, it discusses the methods used by law enforcement to combat these activities. It argues that these spaces should be considered a phenomenon, rather than a natural consequence of technology. The review also proposes a research agenda and serves as a reference document for further exploration of the dark web.*
***Keywords:** dark web, cybercrime, law enforcement, research agenda*

I. INTRODUCTION

The World Wide Web is an information system that allows people from all over the world to exchange information. The Dark Web, sometimes known as the Darknet, is a secret area of the internet. This technology protects users' privacy by encrypting and dispersing their communication over several nodes, making it challenging to track their movements. The Onion Routing (Tor) network and protocol, which have become a hub for many illicit activities including the trafficking of illegal goods and the recruiting of members, is the most widely utilised kind of the Dark Web. Silk Road, a drug market that opened in 2011 and was shut down in 2013, helped the Dark Web acquire prominence. The Dark Web is infamous for enabling illegal activities, and law enforcement agencies are increasingly targeting and monitoring it. The goal of this article is to examine the Dark Web's present condition, development, functions, contribution to cybercrime, and law enforcement initiatives.

The paper begins by introducing the concept of the Dark Web, followed by a discussion of the literature search methodology. The paper then explores the phenomenon of the Dark Web, its major roles, and the legal and societal concerns associated with it.

II. RELATED WORKS

1) "The Darknet and the Future of Content Distribution" by Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman: This paper discusses the motivations behind the creation of the darknet and its potential impact on content distribution. It explores the challenges faced by traditional content distribution models and proposes potential solutions.
2) "The Darknet: A Digital Copyright Revolution" by E. Gabriella Coleman: This book delves into the cultural, political, and ethical implications of the darknet. It examines the underground communities and practices that have emerged within the darknet and how they challenge established notions of copyright and intellectual property.
3) "Exploring the Dark Side of the Internet: A Review of Underground Marketplaces" by Martin Bouchard and Tom Holt: This research paper provides an overview of underground marketplaces operating on the darknet. It explores the types of goods and services exchanged, the structure of these marketplaces, and the challenges faced by law enforcement in combating illicit activities.
4) "The Rise of the Darknet Markets" by Nicolo Zingales and Tommaso Valletti: This paper focuses on the economic aspects of darknet markets, specifically examining the impact of law enforcement interventions on their operations. It discusses the market dynamics, pricing strategies, and customer behavior within the darknet markets.
5) "Mining the Darknet: Drugs, Coins, and Cyber Threats" by Philip O. Gaudette, Robert E. McGrath, and Nicolas Christin: This research paper explores the darknet ecosystem, with a particular emphasis on the trade of illicit drugs and cryptocurrencies. It analyzes the structure of darknet markets, the behavior of vendors and buyers, and the challenges faced by law enforcement agencies.

III. BACKGROUND

People from many nations, ethnicities, and faiths may now communicate with one another thanks to the internet, which has helped to create a global digital society that transcends geographical boundaries. Online identities, like IP addresses, are connected to specific people or websites that control them, thus even if they are amorphous, online actions are nonetheless governed by the laws

©IJRASET: All Rights are Reserved

of the nations in which they take place. Law enforcement may easily monitor online traffic and obtain logs from people who possess it thanks to this degree of culpability. In this topic, the idea of "digital anonymity," or the lack of a connection between a digital identity and a physical one, is essential. The internet may be split into three primary groups based on the characteristics of public vs private and accountable versus anonymous.

First off, since the stakeholders are known, the surface web is more accountable, more open, and accessible without verification or payment. Second, the deep web is secret, not listed by search engines, and not available to the general public. Since access is restricted by internal networks or requirements for authentication, it is still accountable.

The dark web, also known as darknets, is an area of the internet that is not indexed by search engines and requires specialised software to access. It has both public and private components and enables the hosting of hidden services with cloaked IP addresses as well as other anonymous online services.

The absence of accountability distinguishes the dark web most significantly from the other two categories. Because users on the dark web are invisible to the network and anybody monitoring it, their actions are effectively anonymous. The Tor network, the dark web's most flamboyant form, carries internet data through many nodes that are all blind to the traffic's origin and final destination. Since there are no central servers or points of control in this decentralised system, it is difficult to take down the black web.

Universities or human rights advocacy groups give bandwidth to the Tor network in favour of free access. The Tor protocol combines encrypted connections and traffic layering to guarantee anonymity whether using the public internet or visiting sites that are only accessible via the Tor network. The main benefit of using an overlay network like Tor for many users is not simply to visit popular websites invisibly, but also to access a variety of websites that are often inaccessible via the surface web.

IV. RESEARCH METHOD

Conducting a literature review on the dark web poses a major challenge of identifying and organizing relevant literature related to the topic. This was addressed by doing a keyword search with filters on popular databases like EBSCOHost and Google Scholar. The search began with general terms like "dark web" and "dark net," but it was eventually focused on "tor" and "tor hidden services" because it was discovered that this was the most favoured form of the dark web. In order to allow for a more thorough treatment of each aspect of the issue, the search was limited to publications published in the recent five or six years, and additional keywords like "markets," "cybercrime," and "threat intelligence" were included. A total of 189 journal articles, books, and these were recognized and used to create an abstract matrix. After manual filtering, only 41 articles were selected for the final list as they focused specifically on the dark web. However, most of these articles are paramount to the USA, which might result in a favoritism towards that region in the discussion, particularly in relation to civil liberties.

Despite the wealth of information available on the internet, research on the dark web is limited due to its character. Search engines do not display Tor Hidden Services, therefore it is necessary to manually compile a list of "onion" addresses before anybody becomes suspicious. Dark web users are also anonymous, which makes it incredibly challenging to get any type of information about them. The characteristics of traffic flows are still unknown, despite the fact that the Tor Metrices project offers differentiating statistics on Tor usage. The scarcity of published scholarly research on the dark web is a result of these limitations and the specialised software needed to access the network.

V. DISCUSSION OF LITERATURE

The dark web is a distinct aspect of a particular administered network built on top of the worldwide internet, offering the capability of staying hidden and secure from scrutiny, particularly from law enforcement. Recent advancements in technology have enabled new means of supporting and maintaining the dark web for extended periods.

A. Dark Web as a Phenomenon

The dark web, with its promise of remaining incognito and deficiency of traceability, has emerged as an attractive alternative for those seeking to avoid government scrutiny. This is reflected in the diverse range of activities found on the dark web, including illegal marketplaces, social interactions related to training, recruitment, and propaganda, and financial transactions that leave no paper trail. These activities are reminiscent of the features of a black market economy, which emerges as a result of parties engaging in exchange. The dark web can be seen as a digital space that fulfills the requirement for being hidden and invisible among its units, much like a more of a real world black market caters to the nonregulated interchange of goods and services. The dark web's concealed services, particularly those that contain any kind of illegally known content, have become the main cause for the antagonistic relationship between law enforcement agency and the dark web. Law enforcement authorities attempt to cease activity

certain anonymous services or to identify their customers, while participants in this situation try to avoid being detected. Despite the challenges, the shared goal of anonymity and trading has created a worldwide private space that is largely unconcerned about to local jurisdictions. The hiddenness provided by the dark web has given rise to a market-based society that resists external efforts to disrupt it.

B. Major Roles of the Dark Web

Due to its promise of anonymity, the dark web presents opportunity for both legitimate and illicit activity. Protection-seeking people, military usage for anonymous command and authority services, journalists working in nations without free media, and security forces performing dishonest activities are just a few examples of legitimate applications. Contrarily, illegal activities include the use of botnet command and control endpoints, trading in zero-day exploits, hiring hackers, personal communication, coordinating assaults, using botnets to perform Distributed Denial of Service attacks, and dealing in stolen data. The different legal systems in different nations may affect how the dark web is used for legal purposes. Additionally, individuals seeking hiddenness in the physical world can create a figure that appear for them across multiple online services, allowing for a strong and consistent online availability while remaining substantially mobile. This is especially important for avoiding legal prosecution in developed countries, which have a highly collaborative nature.

Tor anonymous services, at least which are connected with a website front, exist in various topics, as shown in a figure with node size proportional to the topic presence and edge weight representing relatedness of the nodes. Overall, the promise of being hidden on the dark web offers both opportunities and challenges, and its use depends on the legal and ethical considerations of individual users.

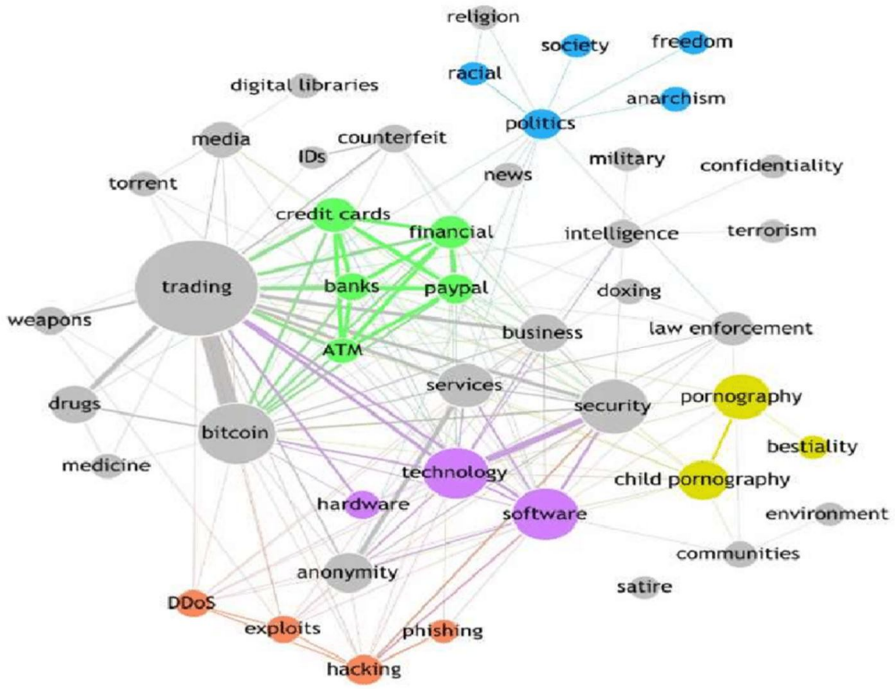


Figure 1: A Taxonomy of Tor Hidden Services.

1) Markets/Illegal Content

Marketplaces like Silk Road, Hansa, and AlphaBay have developed a reputation for facilitating the trading of illegal products, such as several illicit drug varieties, lethal weapons, numerous stolen identities, credit card or debit card credentials, illicit child pornography, and more. With sales of over USD 1.43 million per month, mostly from the selling of drugs and other banned substances, Silk Road was one of the most important and significant of these marketplaces. Although guns are also available on these sites, the sale of illegal narcotics predominates. Another common practise is the sale of stolen data since it gives thieves a way to remain anonymous. Such information may include records relating to financial fraud, such as credit or debit card information, or data that facilitate identity theft, such as medical records, which often have a longer shelf life.

2) Communication and Recruitment

The dark web's hiddenness and unregulated environment attracts malicious actors like hackers and terrorist groups. It provides a platform for anonymous communication, allowing terrorist groups to spread their ideology, recruit members, raise funds, and form communities regardless of geographic limitations or the availability of a local leader. Likewise, hackers can use the dark web to contribute information as an incognito. As a result of its extensive use for such purposes, the dark web forums have been the focus of different types of monitoring, from physical observation to automated threat intelligence using crawling and natural language processing techniques to glean insights.

3) Cybercrime and Terrorism

The dark web is an ideal space for cybercriminals and terrorists due to its deregulated and anonymous nature. Cybercrime can be easily conducted by anyone, and the use of low-risk criminal activities like distributed denial-of-service (DDoS) attacks, which are available through botnets, have become increasingly popular. The incognito services offered by Tor are helpful in international assaults, especially in maintaining communication links between breaches and targets. The ability of nation-states to prepare for digital warfare is a worry, especially when it comes to vital infrastructure and industrial control systems. The asymmetry of the battle environment, where attackers may select their tactics, time, and place, further facilitates this ease of entrance into cybercrime.

In contrast to conventional warfare, where a weapon may be simply written or purchased on the dark web, deterrence and dissuasion do not apply in cyberspace. Governments are no longer the only ones who may use deterrence; non-state entities can also engage in cyberwarfare against shared foes. Though these organisations have moved to the dark web, law enforcement agencies and hacktivist organisations have been active in suppressing terrorist operations on the surface web. Their operations may still be sponsored by virtual currencies there, where their followers can openly voice their thoughts in an anonymous setting, and where they can recruit and train new members. There is an ongoing attempt to use natural language processing to detect terrorist activity on dark web forums. The anonymity offered by the dark web makes it an appealing space for terrorist groups to conduct recruitment activities and spread their ideology. They can communicate anonymously, allocate knowledge, training, advertising, fundraising, targeting, and forming communities without any disquiet for geographical separation or the availability of a local leader. Cybercriminals can also use the dark web to conduct their activities without fear of being caught. They can choose their targets, and the low risk associated with many cybercrimes allows them to engage in criminal activities without fear of severe consequences.

Cybercriminals and terrorists may be able to carry out sophisticated operations including command and control (C2) links between breaches and targets by using Tor's disguised services. Since C2 servers are one of the most well-known anonymous services accessible, Tor's secrecy and resistance to closure make it the ideal platform for them. Critical infrastructure and industrial control systems are impacted by cyber warfare, and nation states are expressing worry about the necessity to prepare for war in the digital sphere, especially when negative real-world consequences are conceivable. In conclusion, the dark web gives malicious individuals a place to engage in unlawful acts, such as cybercrime and terrorism. The dark web is the perfect venue for these operations since it is unregulated and anonymous. Cybercriminals and terrorists may operate with relative ease due to the asymmetry of the wartime environment and the simplicity of admission into the cybercrime world. Although these societies have moved to the dark web, security forces organisations and hacktivist groups are still striving to reduce terrorist activity on the surface web. The identification of terrorist activities on dark web forums is an ongoing effort that requires continued attention.

4) Cyber Threat Intelligence

The dark web is monitored by security agencies and businesses to stay on top of cybercrime activity. Users are safeguarded against malware by antivirus and security companies using historical attack signatures. However, organizations are shifting towards a proactive security approach, integrating Situational Awareness (SA) into their Informational Security Risk Management (ISRM) systems. SA involves collecting and processing data to manage security risks. This has led to the emergence of Cyber Threats Intelligence (CTI) practices, that usually focus on collecting data about cybercriminal activities, especially on dark web meetings.

5) Financial Transactions

As a complement to the anonymous nature of the dark web, cryptocurrencies like Bitcoin have made it feasible to trade money virtually anonymously, enabling untraceable funding of activities. Although Bitcoin offers pseudonymity and makes all transactions connected to an address publicly visible, it is still feasible to use "tumbling" favours on the dark web to launder bitcoin. These services efficaciously make it very hard to connect deposits and withdrawals from a person’s digital wallets to particular transactions that may be undergoing investigation.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Criminals use cryptocurrencies to facilitate payments on dark web marketplaces and to fund illicit activities, such as paying ransomware attackers in Bitcoin in interchange for having their files cracked. While it is possible for a well>resourced assailant to give up the find of Bitcoin<over>Tor users, disrupting the technology itself may not be the most effective approach due to the more upcoming dispensed kind of financial deals and markets. Instead, identifying and prosecuting offenders may be a more effective strategy.

6) Proxy to Surface Web

Besides criminals, the Tor darknet is also utilized by civilians for a variety of reasons. They can use it to access restricted content or websites that may be monitored for privacy and ad tracking concerns. For example, Chinese residents use Tor to evade internet filters imposed by the government, while journalists and whistleblowers use it to communicate sensitive information and avoid legal repercussions. Popular surface web services like Facebook, ProPublica, and DuckDuckGo also have hidden service versions accessible through Tor. These legitimate uses of the Tor network highlight its importance in enabling free speech and access to information.

C. Legal and Societal Concerns

Researchers are actively searching for weaknesses in the Tor network to enable law enforcement agencies to identify users or disrupt their communications. Although several dark web marketplaces have been shut down, new ones often take their place, and fully distributed marketplaces with no central servers have become more established in recent years. Combined with Bitcoin and the Tor protocol, these marketplaces can offer users almost complete anonymity. Passive methods to identify users include fingerprinting circuits set up in Tor connections, looking over traffic within in-between relays or correlating traffic in the middle of entry and exit nodes. Adversaries with nation-state level capabilities can potentially deanonymize almost all Tor traffic within months, while stylometry can link identities across multiple hidden services. By requiring users to connect to attacker-controlled relays, denial of service attacks may also be used to discourage usage or support attempts to remove anomia. Despite the efforts of law enforcement, Tor's creators and maintainers keep updating the software and protocol to address security flaws. Due to their reputation for being more secure than Tor, other networks, such those using Freenet's P2P technology, are also growing in popularity.

VI. RESEARCH AGENDA

The following section highlights gaps in existing literature on the Dark Web and proposes research questions to address these gaps.

A. Enabling Cybercrime: Criminals' Dependence on the Dark Web

Cybercriminals have used the dark web's anonymity to carry out a number of illegal operations, including buying zero-day vulnerabilities, running C34 servers for botnets and malware exfiltration, and hiring out experienced criminals. These actions are carried out by a variety of cybercriminals, from novices to highly organised Advanced Persistent Threat (APT) actors. These APT actors have been responsible for high-profile instances of espionage on significant organisations and nation states, focusing on their digital assets. However, there isn't much work examining the connection between APTs and the dark web. Investigating this connection could help in the future by limiting or improving defences against APT cyberattacks.

B. Distributed Hidden Services & Dark Web Scalability

Hidden services use anonymity on the dark web to hide their actual location and address. It is challenging for law enforcement to shut down these services since the hosting business and location are unclear. As was recently shown, markets on the darknet like Silk Road, Hansa, and AlphaBay are not exempt from regulation. Market place operators are searching for ways to better safeguard themselves as a result. When anonymity is insufficient in these circumstances, a more distributed implementation may be the best option. This solution is now being tested by a number of new decentralised marketplaces that are either built on Tor or blockchain technology. To determine if the current internet infrastructure continues to sustain this phenomenon or acts as a barrier to its use, it is possible to do study on the dark web's scalability. Given that various techniques for eliminating the anonymity of clients or services depend on controlling enough nodes on the Tor network, more study may be done to discover what rate of growth, or user adoption, of Tor is necessary before these approaches become economically impractical to exploit. This study could help law enforcement rethink how it keeps an eye on the dark web.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

C. Role & Capability of Law Enforcement

Advancements in automation have made it progressively challenging for authorities to trail, recognize, and close down sites promoting illegal activities. The decentralization of communication on the dark web has made it harder to regulate, allowing for the expansion of immoral and illegalized content, while increasing the difficulty of keeping track by security forces. In order to prevent the provision of unlawful activities, it is now a top priority for law enforcement to eliminate the anonymity of hidden services, marketplace operations, site administrators, and anyone else involved.

The debate over what can and should be done to regulate technology is a complicated one. Unrestricted and unchecked access to internet technology supports civil freedoms while simultaneously creating a favourable atmosphere for illegal activity. Conversely, policies that restrict the usage of the surface or dark web may infringe on civil liberties. Therefore, initiatives aimed at prosecuting the traders rather than facilitators of the marketplace may be a more viable approach, especially as technological advancements make the latter increasingly difficult.

Some studies propose increasing the frequency of sting operations and focusing on destroying the sources of drugs rather than the market itself as the issue expands over time. However, it is essential to balance the need to curb illegal activities with the protection of civil liberties. Moreover, it is crucial to investigate the effectiveness of various approaches to regulating the dark web, such as legal measures or technological solutions like deanonymization techniques. Further research can explore the ethical implications of regulating the dark web and determine the most effective measures for protecting both civil liberties and society as a whole.

D. Dark Web Phenomenon Growth vs Regulatory Growth

The majority of dark web research focuses on removal of anonymity or threat intelligence. But it's crucial to comprehend the dark web as a manifestation of people looking for discreet places to conduct their business. This viewpoint can assist stakeholders gain greater understanding of the development of the dark web and make more informed decisions, such as investing in more effective monitoring technologies for law enforcement. We contend that as restrictions have expanded and personal freedoms have shrunk, so has the expansion of the dark web. Cybercriminals' use of the dark web to support illegal activity and law enforcement's efforts to stop them can influence technology advancement and growth in a way that benefits unlawful activity especially when this investment is supported by the financial return from such activities. The technical innovation and high level of sophistication of Mexican drug cartels, for instance, is what fuels their expansion.

Future research might look at whether the dark web phenomenon and investments in the technology that makes it possible are expanding over time and if this increase is linked to a reduction in personal liberties or a tightening of regulations. A conversation about the intended effect of policy on the dark web might be sparked by research that demonstrates the relationship between civil liberties legislation and the dark web phenomena. Manipulating civil liberties legislation could have an impact on the intended consequence of the dark web phenomena, for example. Understanding these connections can help policymakers create appropriate regulations for the dark web while also protecting individual freedoms.

VII. CONCLUSIONS

This review paper aims to provide a thorough literature evaluation of the dark web, its function in contemporary digital society, and its effects on society and law enforcement. However, completing a study on this issue was difficult because there isn't much information available about it because it's private and anonymous. The purpose of the dark web today was the first study issue addressed. It was found that the dark web encompasses a variety of other industries as well, including markets for the exchange of software vulnerabilities, the recruiting of extremists, and more.

The relevance of the dark web to cybercriminal operations and activities was the subject of the second study question. According to the analysis, the dark web is utilised for a variety of illegal activities, including functioning as a training ground for online criminals through message boards and hosting facilities for online criminal enterprises. To hide their activities, find their zero-day vulnerabilities, and fund their operations, established and well-resourced actors are thought to employ their own private infrastructure, such as botnet proxies. In essence, the dark web does nothing more than make it easier to commit criminality.

The final study topic concerned the efforts made by law enforcement to stop criminal activities on the dark web. Law enforcement's efforts to shut down businesses that sell illegal goods, notably recreational drugs, are ongoing. However, the infrastructure responds to these events, reducing the weaknesses that the government abused. As a result, market players enhance their operational security, the Tor protocol is continuously upgraded to address weaknesses, and the financial system rolls out newer, more anonymous variations in addition to a surge in services for money laundering. Additionally, distributed hidden services are growing, and escrow functions are expanding to be based on cryptographic advancements rather than merely faith.

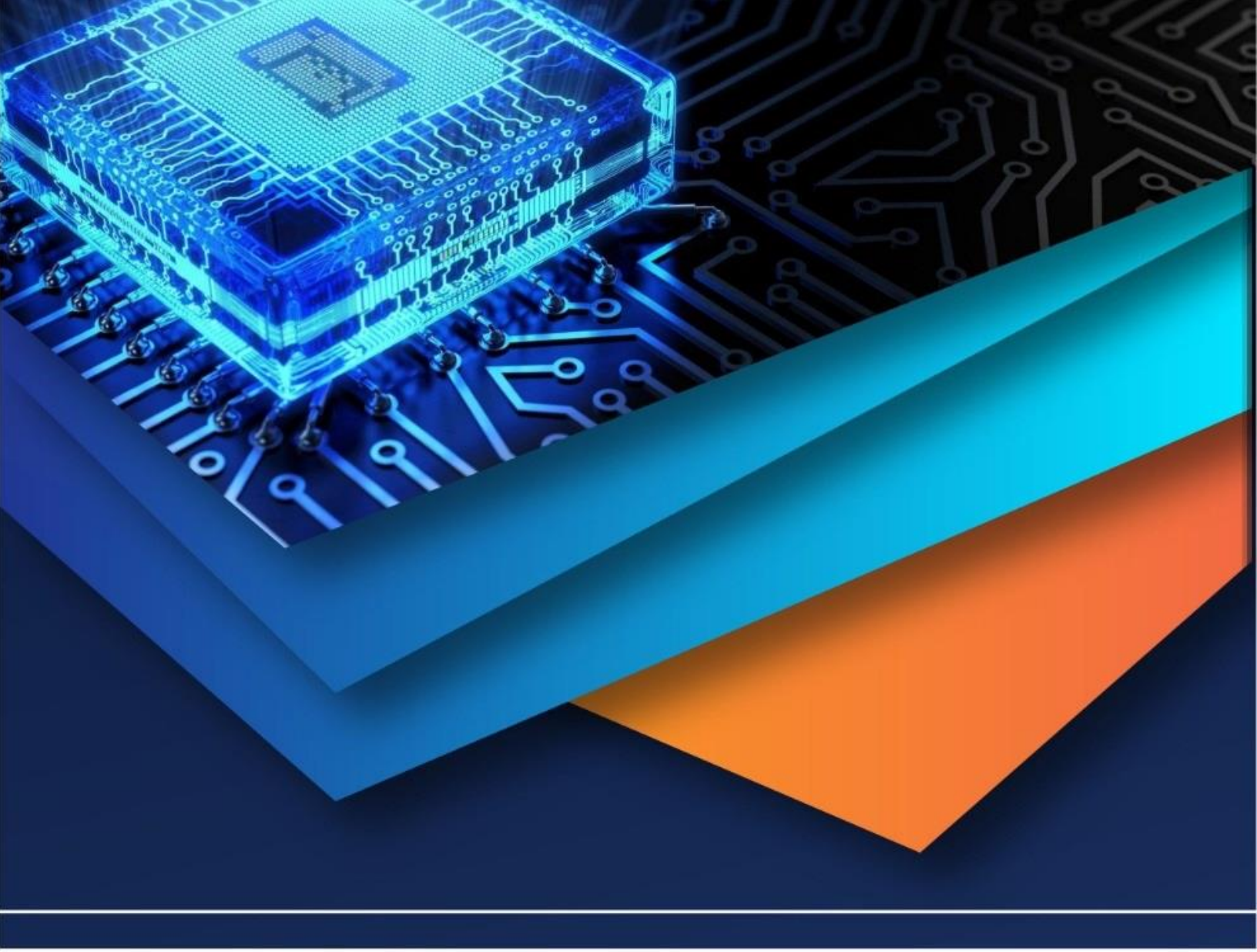
©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Technology is increasingly playing a bigger part in the privacy vs security discussion as it becomes more than simply a legal issue to monitor and spy individuals; it is now a technological one. With the development of technology, it is getting more and harder to find and close down websites that support criminal conduct. The discussion on this issue requires multidisciplinary consideration by authorities in psychology, sociology, law, and other fields because it's probable that it won't only be a technological issue in the future. Instead, it will become an issue of individual freedom of expression and privacy, which can cause moral conundrums in society.

The necessity for multidisciplinary study into the topic is highlighted by this thorough literature review of the dark web, its function in contemporary digital society, and its effects on law enforcement and society. Finding a balance between civil rights and law enforcement is necessary as the dark web develops and presents new difficulties for law enforcement. As it becomes increasingly difficult to oversee technical improvements, the emphasis should be on actions elsewhere in the process, such as punishing the traders rather than the marketplace facilitators.

REFERENCES

[1] Abbasi, A., and Chen, H. 2007. "Affect Intensity Analysis of Dark Web Forums," 2007 IEEE Intelligence and Security Informatics: IEEE, pp. 282-288.
[2] Ablon, L., Libicki, M.C., and Golay, A.A. 2014. Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. Rand Corporation.
[3] Ahmad, A. 2010. "Tactics of Attack and Defense in Physical and Digital Environments: An Asymmetric Warfare Approach," Journal of Information Warfare. (9:1), pp. 46-57.
[4] Ahmad, A., Webb, J., Desouza, K.C., and Boorman, J. 2019. "Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack," Computers & Security).
[5] Biryukov, A., and Pustogarov, I. 2015. "Bitcoin over Tor Isn't a Good Idea," Security and Privacy (SP), 2015 IEEE Symposium on: IEEE, pp. 122-134.
[6] Biryukov, A., Pustogarov, I., Thill, F., and Weinmann, R.-P. 2014. "Content and Popularity Analysis of Tor Hidden Services," Distributed Computing Systems Workshops (ICDCSW), 2014 IEEE 34th International Conference on: IEEE, pp. 188-193.
[7] Broadhurst, R. 2017. "Cybercrime: Thieves, Swindlers, Bandits and Privateers in Cyberspace,").
[8] Broadhurst, R., Woodford-Smith, H., Maxim, D., Sabol, B., Orlando, S., Chapman-Schmidt.
[9] Alazab, M. 2017. "Cyber Terrorism: Research Review: Research Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology,").
[10] Brynielsson, J., Horndahl, Johansson, F., Kaati, L., Mårtenson, C., and Svenson, P. 2013. "Harvesting and Analysis of Weak Signals for Detecting Lone Wolf Terrorists," Security Informatics (2:1), p. 11.
[11] Chertoff, M. 2017. "A Public Policy Perspective of the Dark Web," Journal of Cyber Policy (2:1), pp. 26-38.
[12] Chertoff, M., and Simon, T. 2015. "The Impact of the Dark Web on Internet Governance and Cyber Security,").
[13] Christin, N. 2013. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," Proceedings of the 22nd international conference on World Wide Web: ACM, pp. 213-224.
[14] Crawley, A. 2016. "Hiring Hackers," Network Security (2016:9), pp. 13-15.
[15] Dalins, J., Wilson, C., and Carman, M. 2018. "Criminal Motivation on the Dark Web: A Categorisation Model for Law Enforcement," Digital Investigation (24), pp. 62-71.
[16] Denic, N.V. 2017. "Government Activities to Detect, Deter and Disrupt Threats Enumerating from the Dark Web," US Army Command and General Staff College Fort Leavenworth United States.
[17] DiPiero, C. 2017. "Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web," U. Ill. L. Rev.), p. 1267.
[18] Duddu, V., and Samanta, D. 2018. "Network and Security Analysis of Anonymous Communication Networks," arXiv preprint arXiv:1803.11377).
[19] Fraser, J. 2015. "4 Reasons Why Decentralized Marketplaces Are Inevitable." Retrieved 30/8/18, from https://medium.com/originprotocol/4-reasons-why-decentralized-marketplaces- areinevitable-25b842565e48
[20] Ho, T.N., and Ng, W.K. 2016. "Application of Stylometry to Darkweb Forum User Identification," International Conference on Information and Communications Security: Springer, pp. 173-183.
[21] Hoffman, D., and Rimo, P. 2017. "It Takes Data to Protect Data,").
[22] Jansen, R., Juarez, M., Gálvez, R., Elahi, T., and Diaz, C. 2017. "Inside Job: Applying Traffic Analysis to Measure Tor from Within," Network and Distributed System Security Symposium: IEEE Internet Society.
[23] Jansen, R., Tschorsch, F., Johnson, A., and Scheuermann, B. 2014. "The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network," Office of Naval Research, Arlington. Johnson, A., Wacek, C., Jansen, R., Sherr, M., and Syverson, P. 2013. "Users Get Routed: Traffic
[24] Correlation on Tor by Realistic Adversaries," Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security: ACM, pp. 337-348.
[25] Kwon, A., AlSabah, M., Lazar, D., Dacier, M., and Devadas, S. 2015. "Circuit Fingerprinting Attacks:
[26] Passive Deanonymization of Tor Hidden Services," 24th USENIX Security Symposium. Lautenschlager, S. 2016. "Surface Web, Deep Web, Dark Web -- What's the Difference." Lexie. 2018. "9 Must-See. Onion Sites from the Depths of the Dark Web." Retrieved 30/8/2018
[27] Maddox, A., Barratt, M.J., Allen, M., and Lenton, S. 2016. "Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital 'Demimonde'," Information, Communication & Society (19:1), pp. 111-126.
[28] Mathiassen, L., Saarinen, T., Tuunanen, T., and Rossi, M. 2007. "A Contingency Model for Requirements Development," Journal of the Association for Information Systems (8:11), 569-597.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)