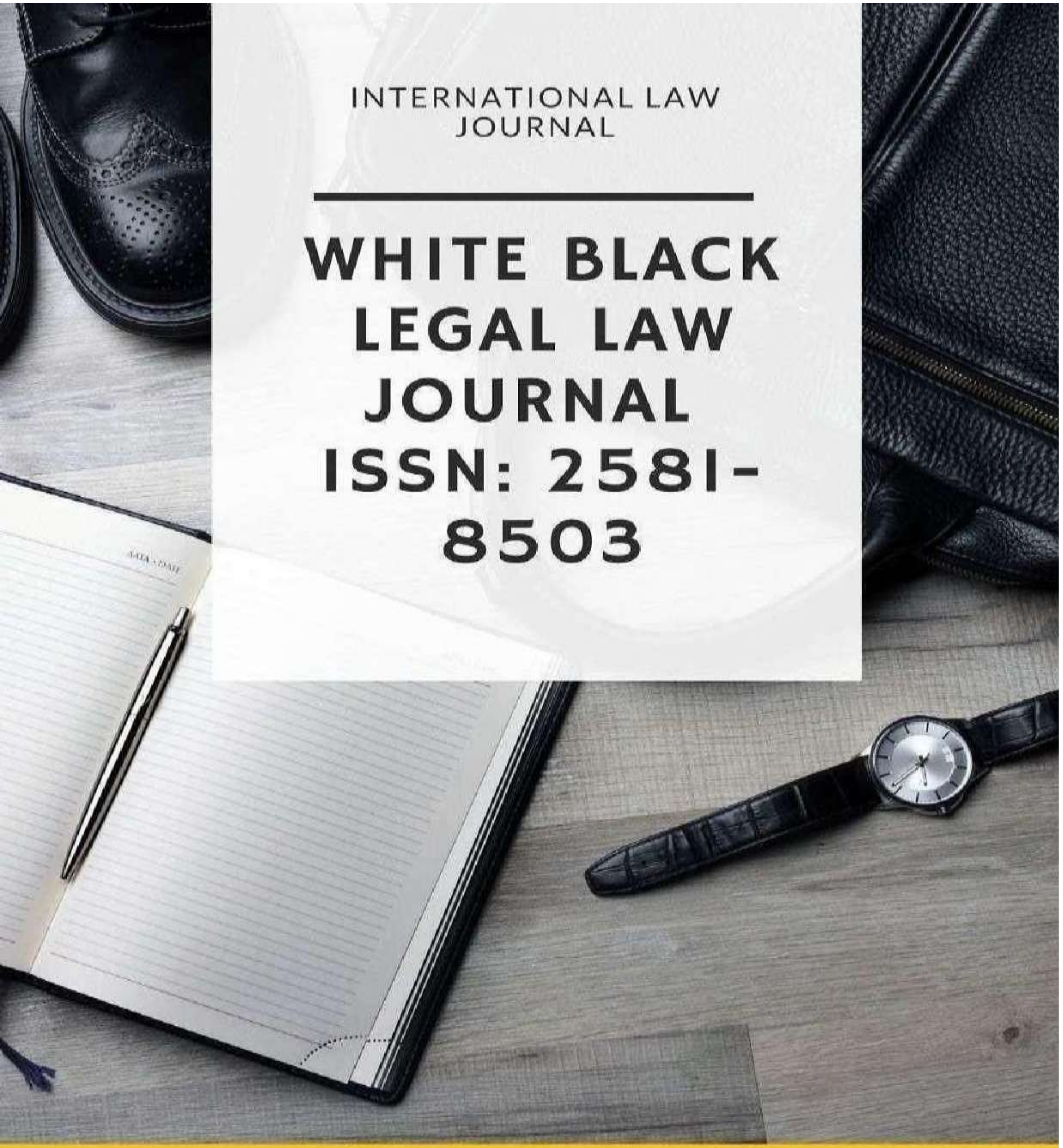

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

NAVIGATING THE SHADOWS: THE DARK WEB'S IMPACT ON MODERN INDIA

AUTHORED BY - ROSHNI PARVEEN & DANIYAL ZAMEER*

Abstract

The dark web, a hidden enclave of the internet accessible only through specialized software, presents a complex landscape of anonymity and criminal activity. This paper explores its nuances, focusing on its use in government, military, and intelligence sectors, as well as its role in illicit transactions such as human trafficking, child pornography, terrorism, drug trafficking, information theft, and financial crimes like money laundering. In the context of India, the dark web poses significant challenges, with criminal activities falling under various legal frameworks. Despite stringent laws, combating these crimes remains a formidable task due to the dark web's encrypted nature and international jurisdictional issues. This paper also examines statistical insights into dark web usage in India and analyzes existing legal measures and their effectiveness. Understanding the dark web is crucial for developing effective strategies to mitigate its risks and protect societal interests. This study concludes by highlighting the need for enhanced international cooperation, technological innovations in cybersecurity, and robust legal frameworks to combat the evolving challenges posed by the dark web in contemporary India.

Keywords: Dark Web, Cybercrime, Anonymity and Privacy

***** LLM, Faculty of Law, Aligarh Muslim University

Introduction

The dark web refers to a clandestine portion of the internet that is not accessible via conventional search engines. By transmitting user data over a network of encrypted nodes, it offers a level of security against unauthorized access, but can only be accessed using specialized software like Tor. A wide range of users are attracted to this anonymity, including activists seeking to evade censorship as well as cybercriminals engaged in illicit business, financial deception, and the trade of weapons and narcotics.

The dark web serves as a sanctuary for illicit endeavors, notwithstanding its promotion of anonymity. The dark web marketplaces worsen the worldwide issue faced by law enforcement organizations by facilitating the exchange of illegal goods and services. The dark web has genuine applications that extend beyond its negative associations, including the use of encryption for secure communication and the interchange of data in environments governed by totalitarian regimes. To strike a balance between these two conflicting objectives, one must possess knowledge of the dark web to navigate its complexities and minimize its impact on global cybersecurity and law enforcement efforts.

Understanding Dark Web

The dark web is a secret section of the internet deliberately concealed and unattainable using conventional web browsers. Contrary to the surface online, which is searchable by search engines like Google, the dark web necessitates specialized software, such as Tor (The Onion Router), for entry. This network ensures anonymity by using a series of encrypted nodes to route user data, making it arduous to track the source or destination of the information. This high degree of secrecy appeals to a diverse range of users, including activists and journalists in repressive regimes who want safe communication, as well as cybercriminals who aim to participate in illegal activity.[1]

Although the dark web provides a sanctuary for unrestricted expression and confidentiality, it is also well known for facilitating illicit endeavors. Dark web online marketplaces often enable the exchange of illicit commodities and services, such as narcotics, firearms, forged currency, and pilfered information. Law enforcement authorities globally persistently strive to counteract

[1] Encryption in Wireless Network, *available at:* https://www.open.edu/openlearn/mod/oucontent/view.php?id=48321&section=2.2 (last visited on June 14, 2024).

these illicit activities, although the obscurity of the dark web presents substantial obstacles. Although often linked to illicit activity, the dark web also fulfills lawful functions. Whistleblowers use it as a means to disseminate sensitive information without fear of reprisal, while also serving as a platform for unrestricted speech in nations with stringent censorship regulations. In addition, cybersecurity experts use the dark web to surveil risks and collect information on prospective security breaches. The dark web is an intricate and diverse section of the internet that encompasses both the advantageous and detrimental qualities of anonymity and privacy.[2]

History of Dark Web

The first phase of development in the history of the internet and related technologies can be traced back to the 1960s, as outlined in the first table. This era saw the initiation of ARPANET by the U.S. Department of Defense, led by the Advanced Research Projects Agency (ARPA). ARPANET was revolutionary, introducing the concept of a packet-switching network that enabled the connection of multiple computers, thus facilitating remote communication and resource sharing. The 1970s marked ARPANET's operational phase, predominantly for academic and research purposes. Notably, this decade also witnessed the first illegal online transaction involving the sale of marijuana, signaling the nascent stages of e-commerce, albeit illicit. "The 1990s were pivotal with the research and development of Onion Routing by the U.S. Naval Research Laboratory, laying the groundwork for anonymous communication and eventually leading to the creation of Tor."[3] The 2000s saw the completion and initial release of Freenet, aimed at providing decentralized internet solutions, followed by the release of Tor in 2002, which quickly gained traction among privacy advocates and researchers. The release of Bitcoin in 2009 by Satoshi Nakamoto introduced the first decentralized cryptocurrency, further advancing the capabilities and reach of online transactions.

Year	Development
1960s	❖ U.S. Department of Defense initiates ARPANET ❖ Advanced Research Projects Agency (ARPA) leads project ❖ Development of packet-switching network ❖ Connection of multiple computers

[2] Journalism and whistleblowing: an important tool to protect human rights, fight corruption, and strengthen democracy, *available at:* https://unesdoc.unesco.org/ark:/48223/pf0000381406 (last visited on June 14, 2024).

[3] *Ibid*

	❖ Enables remote communication and resource sharing
1970s	❖ ARPANET was operational and primarily used for academic and research purposes. ❖ The first illegal online transaction involved the sale of marijuana. ❖ Students at Stanford University and MIT conducted the transaction. ❖ ARPANET facilitated communication and coordination for the sale. ❖ This event marked the earliest known instance of e-commerce, albeit illegal.
1990s	❖ Research and development of Onion Routing began. ❖ Concept of anonymous communication over a computer network established. ❖ Prototype of Onion Routing created by U.S. Naval Research Laboratory. ❖ Initial testing and refinement of the routing protocols. ❖ Foundation laid for the future development of Tor.
2000	❖ Development of Freenet completed. ❖ Initial release of Freenet. ❖ Early adoption by users seeking decentralized internet solutions. ❖ Open-source contributions began. ❖ Growth of Freenet community and network.
2002	❖ Initial release of Tor (The Onion Router). ❖ Developed by the U.S. Naval Research Laboratory. ❖ Aimed to provide anonymous communication over the internet. ❖ Early adoption by privacy advocates and researchers. ❖ Tor Project established to maintain and advance the network.
2009	❖ Bitcoin was released by Satoshi Nakamoto. ❖ The Bitcoin network went live with the mining of the genesis block. ❖ Introduction of the first decentralized cryptocurrency. ❖ Bitcoin software made available as open-source. ❖ Early adoption by cryptography enthusiasts and developers.

The second phase of development, encapsulated in the second table, delves into the more controversial and darker aspects of the internet's evolution. This period, beginning in the 2010s, is marked by significant socio-political events and the rise of darknet markets. The Arab Spring in 2010 highlighted the power of the internet in mobilizing social movements, although it also underscored the instability it could precipitate. In 2011, Ross Ulbricht launched Silk Road, the first modern darknet market, which facilitated anonymous transactions for illegal goods using Bitcoin, accumulating over $1.2 billion in sales before its shutdown by the FBI in 2013. This event spurred the emergence of other darknet markets, perpetuating the cycle of illegal online trade. The dark web's notoriety grew with events like the takedown of Playpen in 2015, a major dark website for child pornography, and the widespread WannaCry ransomware attack in 2017, attributed to the North Korean Lazarus Group. These developments highlight the dual-edged nature of technological advancements, bringing about both innovation and significant ethical challenges.

Year	Development
2010	❖ Began with protests in Tunisia against unemployment, high food prices, and political repression ❖ Spread to other Arab countries like Egypt, Libya, Yemen, Syria and Bahrain ❖ Led to the overthrow of long-standing authoritarian rulers in Tunisia, Egypt, Libya and Yemen ❖ Sparked civil wars and armed conflicts in Syria, Libya and Yemen ❖ Ultimately failed to bring about stable democracies in most countries due to violent crackdowns, civil wars and the rise of extremist groups
2011	❖ Ross Ulbricht launched the Silk Road, the first modern darknet market, allowing anonymous buying and selling of illegal goods. ❖ Ulbricht operated the site under the pseudonym “Dread Pirate Roberts”. ❖ Silk Road transactions were conducted using Bitcoin, facilitating over $1.2 billion in sales from 2011-2013. ❖ The site generated $80 million in commissions for Ulbricht before being shut down by the FBI in 2013. ❖ Ulbricht was arrested, convicted on multiple charges, and sentenced to life in prison without parole
2013	❖ FBI shut down Silk Road, the first modern darknet market

	❖ Operated by Ross Ulbricht under "Dread Pirate Roberts" ❖ Facilitated $1.2B in illegal transactions, $80M in commissions ❖ Ulbricht arrested, convicted on money laundering, drug charges ❖ Other darknet markets emerged to replace Silk Road
2015	❖ Playpen, a dark website for child pornography, was shut down in 2015. ❖ The site had over 215,000 users and hosted 23,000 child abuse images. ❖ The FBI seized control of Playpen and continued to operate it for 13 days. ❖ During this time, the FBI used malware to hack users' computers and collect IP addresses. ❖ The operation led to the arrest of 956 users and five prison sentences.
2017	❖ The WannaCry ransomware attack occurred on May 12, 2017. ❖ It affected over 200,000 computers in 150 countries. ❖ The attack exploited a vulnerability in Microsoft Windows. ❖ It used Eternal Blue and Double Pulsar exploits to spread. ❖ The attack was attributed to the North Korean Lazarus Group.

Role of Dark Web for Government, Military and Intelligence

Due to the anonymity offered by Tor and other tools like I2P, the Dark Web may serve as a platform for malicious individuals on the internet. Although it should be acknowledged, “there are certain domains in which the examination and use of the Dark Web might provide advantages. This is true not only for individuals and companies desiring internet confidentiality, but also for certain branches of the government, including the law enforcement, military, and intelligence sectors.”[4]

Utilizing anonymity on the Dark Web may serve as a means to protect military command and control systems deployed in the field from being identified and hacked by enemies. The military may use the Dark Web to analyze the operational environment and identify actions that pose a potential threat to personnel. For example, there is evidence indicating that the Islamic State (IS) and its affiliated organizations want to use the anonymity provided by the Dark Web for purposes more than only exchanging information, recruiting, and spreading

[4] *Supra Note 1 at page 2.*

propaganda. They employ Bitcoin as a means to generate funds for their operations. The Department of Defense (DOD) may surveil these actions and use a range of strategies to thwart terrorist plans in its fight against IS. “The military may use TOR software for conducting covert computer network operations, such as executing website takedowns or denial of service attacks, as well as intercepting and obstructing enemy communications. Another potential use is in the realm of military deception or psychological operations, when the armed forces leverage the Dark Web to disseminate false information on troop movements and targets, for the purpose of counterintelligence or to undermine the credibility of rebel narratives. These efforts might be carried out either to assist a current military operation or as independent operations.”[5]

The Intelligence Community (IC) openly utilizes the Dark Web as a source of open intelligence, similar to the military. However, specific facts about its use are classified. “Admiral Mike Rogers, the Director of the National Security Agency (NSA) and Commander of U.S. Cyber Command, said that their primary focus is on locating those who actively evade detection. An inquiry into the NSA’s XKeyscore program, which was exposed by Edward Snowden’s disclosure of classified information, revealed that any user trying to download TOR was electronically fingerprinted, potentially enabling the agency to identify users who think they are untraceable.”[6]

Although the particular actions carried out by intelligence agencies on the Deep Web and Dark Web are often kept secret, it is known that the Intelligence Advanced Research Projects Activity (IARPA) has a program that focuses on looking for material stored on the Deep Web. Allegedly, traditional methods like signature-based detection fail to enable experts to predict cyber threats. Consequently, authorities are reacting to, rather than foreseeing and managing, these assaults. “The objective of the Cyber-attack Automated Unconventional Sensor Environment (CAUSE) initiative is to create and evaluate novel automated techniques for predicting and identifying cyber-attacks with greater timeliness compared to current approaches. Actor behaviour models and black market sales may be used to enhance the prediction and identification of cyber incidents.”[7]

[5] Cyber offence in the context of military operations, *available at:* https://www.orfonline.org/expert-speak/cyber-offence-in-the-context-of-military-operations (last visited on June 19, 2024).

[6] Edward Snowden: Leaks that exposed US spy programme, *available at:* https://www.bbc.com/news/world-us-canada-23123964 (last visited on June 19, 2024).

[7] *Ibid*

Mode of Transaction in the Dark Web

Bitcoin is the predominant money used for transactions on the Dark Web. It is a distributed digital money that employs anonymous, peer-to-peer transactions. People often acquire bitcoins by taking them as payment, converting them into conventional cash, or engaging in the process of “mining” them. “Whenever a bitcoin is used in a financial transaction, the details of the transaction are documented in a publicly accessible ledger known as the block chain. The data stored in the blockchain consists of the bitcoin addresses belonging to the sender and receiver. An address does not uniquely designate any one bitcoin; instead, it only designates a certain transaction.”[8]

Users’ addresses are linked to and saved in a wallet. The wallet stores a person’s private key, which is a confidential numerical code that grants the individual the ability to use bitcoins from the associated wallet, much like a password. Transactions are verified using both the address for a transaction and a digital signature. The wallet and private key are not stored in the public ledger, which enhances the anonymity of bitcoin use. Wallets may be stored online, using software on a computer or mobile device, or on a physical hardware device

Crimes In The Dark Web

The proliferation of anonymity-enabling technology has led to a surge in cybercrimes, with the dark web serving as a sanctuary for illegal activities. A substantial proportion of the traffic on the dark web consists of illicit activity. Most Tor users are likely seeking to conceal their online identities or participate in legal online activities. The problem lies with the minority of Tor users who access the Dark Web. Developing a system that both protects users’ online identities and monitors their browsing activities to prevent them from visiting harmful websites is an extremely challenging endeavor. Contrary to the claims of Tor’s creators, the bulk of Tor traffic does not originate from brave journalists operating in countries with limited freedom of expression laws. “People use various web browsers to access clandestine Dark Web sites primarily for the purposes of purchasing illicit narcotics and seeing explicit images of child abuse. Dr. Gareth Owen and Nick Savage from the University of Portsmouth conducted a thorough analysis on the use of Tor and hidden services over a period of six months.”[9] Their findings revealed that identified child abuse websites constituted more than 80% of the Tor

[8] Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stanford Law Review (2017).

[9] The Tor Dark Net, *available at:* https://researchportal.port.ac.uk/en/publications/the-tor-dark-net (last visited on June 19, 2024).

traffic requests sent towards the hidden sites that were investigated. Government agencies sometimes use automated computers to scan websites that include images of child abuse. However, they concede that the data obtained from these scans may not be completely accurate. It is very challenging to determine the proportionate distribution of police activity in relation to unlawful internet trading. A significant volume of user activity on the Dark Web remains focused on child abuse websites, despite the fact that law enforcement intervention is estimated to contribute to half of the observed activity. Photos of child abuse may be found on the Dark Web. The level of activity on the dark web surpasses that of other online platforms.

A: Human Trafficking And Sex Trafficking

Slavery, also known as human trafficking, is a persistent infringement of human rights that affects a vast number of individuals worldwide. In the modern age, around 40.3% of the global population was considered to be in a state of enslavement. Within the realm of the sex trade, several manifestations of human trafficking exist, such as involvement in prostitution and pornography. Similarly, the food and drink industry, street gangs, and the drug trade are other arenas where trafficking occurs, among others. The complexity of human trafficking has increased over the last decade as a result of the proliferation of online platforms and the predominance of covert operations. Due to technology improvements and globalization, it has become more convenient to access a wide audience and use their potential. Human trafficking encompasses several subcategories, such as sex trafficking, labour trafficking, organ trafficking, and newborn trafficking, among numerous others. "Transplantation tourism" on the dark web refers to the act of bringing organ donors to the locations of patients in order to directly remove the organs. "According to Global Financial Integrity 2017, the illegal trafficking of organs produces annual profits ranging from $840 million to $1.7 billion. Another flourishing industry that involves the illegal trade of human beings is the adoption of newborns."[10] Industrial vaginal harvesting, sometimes known as "baby factories," is the exploitation and enslavement of young women for the purpose of producing children for financial gain. Although the darknet claims to prioritize anonymity, these mechanisms effectively assist human traffickers while protecting users from law enforcement. Various research and articles have shown that Darknet facilitates criminal activities via the use of substandard protocols, anonymous IP assignments, peer-to-peer content sharing platforms, and

[10] Organ Trafficking: The Unseen Form of Human Trafficking, *available at:* https://www.acamstoday.org/organ-trafficking-the-unseen-form-of-human-trafficking/ (last visited on June 26, 2024).

untraceable money transactions. On the Darknet, cryptocurrencies such as Bitcoin facilitate the payment for illicit services. The criminal element is taking advantage of these criminogenic features present on the Darknet.

The Human Experiment website details upsetting instances of medical exploitation in which homeless individuals, who were already at a disadvantage, were voluntarily or involuntarily exposed to tests. Someone apparently targeted these individuals and subjected them to a slew of medical procedures, some of which were fatal, since they lacked the necessary paperwork or social protections. These claims are highly troubling, but it is not certain whether the website really exists or if the accountants who worked on it were truthful. After 2011, the website fell offline, thus we have no idea who participated in the trials or whether the information is accurate.

B: Child Pornography

Malefactors and those with deviant sexual interests often use the dark web as a means to disseminate explicit material involving minors. Most individuals who visit underground child pornography sites use Tor. Freedom Hosting has allocated around five hundred and fifty servers across Europe just for the hosting of child pornography. Additionally, it generates revenue from the live exploitation of children via its video streaming applications. Child prostitution via webcam is another use of Voice over Internet Protocol (VoIP). The sale of victims' images online as a consequence of child sexual abuse is an alarming issue. The 2018 breach of the largest child pornography website, known as "welcome to video," situated in South Korea, led to the apprehension of several persons worldwide. In 2018, a total of around 144,000 individuals from the United Kingdom had the ability to see explicit material on the dark web.

C: Terrorism And Arms Trafficking

The dark web facilitates illicit transactions involving firearms. Although crimes on the dark web are generally extensive, the magnitude of the danger posed by weapons trafficking to global security is far greater. Europe, Denmark, and Germany dominate the dark web market for weaponry. Terrorist organizations and people working on the dark web pose significant threats to global security. Terrorist organizations such as Al-Qaeda and ISIS have disseminated their animosity and extremist ideology worldwide by using the dark web. In addition, they acquired funds, procured armaments, indoctrinated fresh recruits, spread propaganda, and orchestrated acts of terrorism worldwide via the use of the dark web.[11]

On the Assassination Market, a website that also serves as a prediction market, users may place bets on the estimated time of a given person's death. If the chosen date coincides with the actual death, the better is paid out. There is financial motivation for the assassins to carry them out if they are able to predict the victim's death with any degree of accuracy. Because the prize in this market is based on predicting the date rather than actually murdering the victim, it is quite difficult to identify the perpetrator. The Dark Web's anonymity and encryption have enabled a troubling increase in the usage of sites like White Wolves and C'thuthlu, where users may engage in the practice of hiring assassins.

D: Drug Trafficking

The act of purchasing and selling illegal drugs is made easier by a wide range of websites available on the dark web. Within the realm of the dark web, there are two separate and discernible platforms dedicated to the illicit trade of narcotics. The drugs market offers a range of illicit substances, such as cannabis, cocaine, psychedelics, and tobacco, that may be purchased. Another option is the general shops, which provide a variety of pharmaceuticals and substances for purchase. "The dark web enables the exchange of illegal drugs in exchange for digital cash. The Silk Road was a legendary drug bazaar that facilitated the trade of drugs worth over one billion dollars. It was closed in 2013. Nevertheless, illicit substances are still being sold via anonymous internet marketplaces such as Mr. Nice Guy, Dream Market, Wall Street Market, Valhalla, and several others. When it comes to searching for drugs on the dark web, "Grams," with a logo that resembles Google's, is by far the most popular."[12] Through the Dark Web, a decentralized marketplace powered by bitcoin, buyers and sellers may evade the usual scrutiny of government authorities. Legendary dark web markets like Silk Road, Alpha Bay, and Dream Market are infamous for selling narcotics, weapons, and even endangered species. These sites use encrypted networks to secure users' identities and financial activities. They also give pictures and short descriptions of products, much like Amazon, Flipkart, and similar sites.[13]

[11] General Assembly, *The United Nations Global Counter-Terrorism Strategy*, UN GAOR, UN Doc Resolution 60/288 (2006).

[12] Drugs and the Darknet, *available at:* https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf (last visited on July 06, 2024).

[13] *Ibid.*

E: Information Leakage and Theft of Intellectual Property

Regarding the theft of sensitive information, there are two primary forms of criminal activity: hacking and data trafficking. The dark web offers a secure platform for hackers to disclose confidential and delicate information. Groups of people with similar interests, ranging from hackers to gamers, have the potential to expand rapidly. Doxing refers to the act of hackers revealing the true identify of an adversary by publicly disclosing it. Nevertheless, those with malicious intent are not the only perpetrators of doxing, which involves the disclosure of personal and confidential data. Hackers see companies, prominent individuals, and public figures as legitimate targets. The ultimate objective remains consistent: attaining fame, wealth, and other such achievements. Wikileaks serves as a prominent example, since it not only operates on the Deep Web, but also offers a platform for the anonymous submission of recent revelations. Although the selling of hacked accounts has been present on the dark web for some time, it is becoming prevalent in that realm. The websites mostly provide accounts from several businesses such as banking, online auctions, gambling, and credit cards. While fees may differ across different regions on the internet, PayPal accounts are generally affordable. Depending on the vendor, these accounts may be available either as high-quality, authenticated statements with a confirmed balance or as substantial volumes of unconfirmed reports. In 2017, the dark web traded more than 1.4 billion distinct records.[14]

The advent of the internet has transformed the dissemination of knowledge and offered up new possibilities for collaboration and innovation. Notwithstanding these benefits, the growth of the dark web has given rise to a secretive underworld where IP theft and other illegal activities thrive. The anonymity and security features of the dark web make it an ideal environment for criminal enterprises to thrive. Within this shadowy realm, con artists engage in a wide variety of illicit activities, including the sale and distribution of stolen intellectual property. Intellectual property includes patents, trademarks, copyrights, and trade secrets, all of which are vital to individuals and businesses. Piracy of digital property, including software, movies, and music, is rampant on underground markets and forums, cutting into the profits of content creators and right holders. Theft of intellectual property on the dark web has a severe effect on businesses, manufacturers, and consumers. Theft of intellectual property is a major threat to businesses' ability to compete since it may lead to the duplication of products, price cuts, or the production

[14] The State of Ransomware in 2022, *available at:* https://www.blackfog.com/the-state-of-ransomware-in-2022/ (last visited on July 06, 2024).

of fake goods, all of which can damage a company's brand and market share. Financial losses caused by intellectual property theft may deter investment in research and development and innovation, which in turn reduces the likelihood of long-term growth and sustainability.

F: Malware/Ransomware

The synergy between malware and the deep web makes it an ideal platform for hosting command and control (C&C) servers. One notable advantage of Tor or I2P is the use of robust encryption to conceal the whereabouts of servers. Forensic investigators are unable to use conventional investigative techniques in this scenario, such as locating the IP address of a server or validating its registration details. Tor is also used for command and control (C&C) operations by several hackers. Some well-known malware families use Tor for certain configurations by including the official Tor client into their setup files. Initially reported in a 2013 article by Trend Micro, this phenomenon took place when the MEVADE virus led to a significant increase in Tor traffic as users started utilizing Tor-hidden services for command and control purposes. Initially, phishing emails served as a means for the dissemination of the VAWTRAK financial Trojan. The IP addresses of the command and control servers are acquired via retrieving an encrypted icon file (favicon.ico) from Tor-hosted websites that are programmed into each instance. Although this strategy effectively hides the location of a criminal server, it exposes its users to potential attacks. Since their computers are already infected with malware, this should not pose an issue. The crypto locker family is an additional instance of malware that takes use of the dark web. Crypto Locker, a kind of ransomware, encrypts the papers of its victims and then redirects them to a malicious website. Hence, payment must be made prior to obtaining access to these materials. Due to its automated detection of various areas and languages, it is evident that the design is well-executed.[15] The deep web's attractiveness to hackers is due to the simplicity with which they may enhance the resilience of their infrastructures against prospective takedowns. The incidence of ransomware attacks is increasing, leading to the creation of several detection engines to aid in the identification of compromised data. Regrettably, it is not possible to retrieve data from a contaminated file, even after the file has been eliminated.[16]

[15] CryptoLocker: Everything You Need to Know, *available at:* https://www.varonis.com/blog/cryptolocker (last visited on July 09, 2024).

[16] *Ibid.*

G: Bitcoin And Money Laundry

Bitcoin is a decentralized cryptocurrency that places a high emphasis on safeguarding user anonymity. Even for illegal transactions, it has grown widespread and well acknowledged. Crypto wallets need users to authenticate their identity, despite the fact that Bitcoin transactions are inherently anonymous. Bitcoin transactions are transparent and may be scrutinized by investigators in accordance with the blockchain architecture. Thus, however not uncomplicated, overseeing finances is definitely achievable. The objective of including several anonymizing services is to enhance the difficulty of tracing bitcoins. Primarily, this is achieved via the process of "mixing" bitcoin, which entails sending and receiving it across a network of small transactions until it ultimately reaches its original owner. Using this approach, the proprietor obtains the monies with little chance of retrieval, and just a fraction is deducted as a fee. Laundry services enhance the anonymity of money transactions performed via the Bitcoin system. Various anonymous services, like Western Union, PayPal, and ACH, are included into the deep web.

Statistics On the Usage of the Dark Web in India

The number of dark web users in India surpasses the total number of dark web users in South America and Australia. Approximately 26 percent of the Indian population use the dark web. An anonymous hacker gang known as Shiny Hunters allegedly attempted to sell the personal information of 73 million individuals on the Dark Web, as reported by ZDNet. Approximately 10 firms had a breach in their security as a result of it. Included on the list were the South Korean fashion website Social Share, the online dating platform Zoosk, and the publishing firm Chat books. In April 2020, Cyble, a cybersecurity firm, disclosed that hackers traded over 500,000 hacked Zoom accounts for a price of less than one rupee per account. According to Arxiv, the proportion of women using the dark web was just 29.4%, whilst males constituted around 70.6% of the users. According to Arxiv statistics, the dark web is used by 35.9% of individuals aged 18–25, 34.8% of individuals aged 26–35, 16.8% of individuals aged 36–45, 8.8% of those aged 46–55, 3.1% of individuals aged 56–65, and 0.6% of individuals aged 65 and above.

Indian Laws and the Dark Web

Crime on Dark Web	Laws related to these crime
Human Trafficking And Sex Trafficking	Section 143 of the "Bhartiya Nyay Sanhita, 2023"[17], as well as under the "Immoral Traffic (Prevention) Act, 1956"[18] (ITPA) and the Protection of Children from Sexual Offences (POCSO) Act, 2012.
Child Pornography	Section 14 of "Protection of Children from Sexual Offences (POCSO) Act, 2012"[19], Section 67B of the "Information Technology (IT) Act, 2000"[20].
Terrorism And Arms Trafficking	"Unlawful Activities (Prevention) Act, 1967"[21] (UAPA) and the Arms Act, 1959, Section 66F of "Information Technology (IT) Act, 2000" and Section 147 of "Bhartiya Nyay Sanhita, 2023".
Drug Trafficking	Section 248 of the "Narcotics and Psychotropic Drugs Act 1985"[22].
Information Leakage and Theft of Intellectual Property	Sections 43 and 66 of Information Technology (IT) Act, 2000, Section 303 of Bhartiya Nyay Sanhita, 2023 and the "Copyright Act, 1957"[23].
Malware/Ransomware	Sections 66 of Information Technology (IT) Act, 2000
Bitcoin And Money Laundry	"Prevention of Money Laundering Act (PMLA), 2002"[24]

The Indian law enforcement has distinct challenges as a result of the country's legislative authorization to browse the dark web. Moreover, India's internet regulations lack stringency. The dark web poses unique challenges as a result of the many regulatory loopholes in our country. India's Information Technology Act of 2000 specifically covers cybercrime in just six sections.

[17] Act 45 of 2023.

[18] Act 104 of 1956.

[19] Act 32 of 2012.

[20] Act 21 of 2000.

[21] Act 37 of 1967.

[22] Act 61 of 1985.

[23] Act 14 of 1957.

[24] Act 15 of 2003.

Sections 98 and 99 of the Bhartiya Nyay Sanhita pertain to the regulation of females who are sold or purchased for the explicit intention of engaging in prostitution. We acknowledge the presence of these illicit operations. They engage in human trafficking, either via direct involvement or indirect means. Human trafficking is a criminal offense.

Individuals involved in the illicit trade of narcotics outside of India may be subject to legal action under Section 248 of the 1985 Narcotics and Psychotropic Drugs Act. Although the dark web itself is not intrinsically criminal, the activities you engage in while utilizing it are undoubtedly unlawful. For instance, engaging in the illicit trade of narcotics with individuals on the dark web might result in severe repercussions. Recall the occurrence in which five students were detained once again for purchasing LSD dots. "Sections 14 and 15 of the POCSO Act of 2012"[25], prohibit the dissemination of child pornography. The particular charges of child pornography are handled only in these sections.

The regulations pertaining to offenses committed against underage females are explicitly stated in the Bhartiya Nyay Sanhita, 2023. Under Section 87 of Bhartiya Nyay Sanhita, if someone incites, coerces, or seduces a juvenile girl into engaging in non-consensual sexual intercourse, they may be punished with a fine and a jail sentence of up to 10 years. Although the dark web itself is not intrinsically criminal, the activities you engage in while utilizing it are undoubtedly unlawful. For instance, engaging in the illicit trade of narcotics with individuals on the dark web might result in severe repercussions.

The Constitution of India specifically prohibits the trafficking of human people or their forced labour.[26] Section 61 of the Bhartiya Nyay Sanhita criminalizes the act of conspiring. Both the Prevention of Terrorism Act of 2002 and the Unlawful Activities (Prevention) Act (UAPA) criminalize and impose penalties for offenses related to terrorism. Counterfeiting Indian money is considered a criminal offense under Sections 178, 179, 180, 181 of the Bhartiya Nyay Sanhita. According to the Bhartiya Nyay Sanhita, murder (Section 103), injury (Section115), and grave harm (Section 131) are all subject to punishment. Extortion (Section 308) and rape (Section 64) are punishable under Bhartiya Nyay Sanhita.

[25] *Supra* Note 19 at 17.

[26] The Constitution of India, art. 23.

Conversely, the Dark Web is not explicitly prohibited by legislation. Offenses related to the dark web are covered by many laws, such as the Bhartiya Nyay Sanhita, the Information Technology Act of 2000, the Indian Constitution, the POSCO Act, UAPA, and POTA. As networks expand, it is imperative to establish robust regulations to identify and apprehend criminals operating via routers.

Challenges of the Dark Web in Modern India

The dark web presents significant challenges for contemporary India, particularly in the domains of cybersecurity and law enforcement. The dark web has emerged as a refuge for several illicit activities because to the anonymity it provides. These activities include the illegal transportation and distribution of drugs, firearms, forged currency, and pilfered information. The Indian authorities have challenges in effectively addressing these crimes because to the elusive nature of underground marketplaces, which makes detection and punishment difficult. Safeguarding the nation and shielding vulnerable populations from perils such as human trafficking, unlawful pornography dissemination, and the solicitation of contract killers on the dark web is already a formidable challenge.

The cybersecurity landscape in India faces significant threats from both traditional criminal activities and the dark web. Cybercriminals on the dark web arrange ransomware attacks, the selling of malicious software, and the transfer of confidential information, including bank data and personal details of Indian people. These acts pose a threat to both the financial sector and national security, while also infringing upon people' right to privacy. With the increasing frequency of assaults against Indian firms, government institutions, and critical infrastructure via the dark web, it is imperative to have a robust and well-coordinated approach to protect sensitive data and ensure uninterrupted operations.

The concealed nature of the internet and the inherent anonymity of its users make it difficult for Indian law enforcement and cybersecurity groups to effectively address dark web operations. To effectively address the threats posed by the dark web, it is imperative to bolster technological skills and establish strong partnerships with foreign law enforcement agencies. In order to further mitigate risk, it is essential to enforce stringent cybersecurity measures and promote public awareness initiatives. Nevertheless, to effectively address these intricate issues, Indian authorities must consistently modify and enhance their rules in order to counteract the continuously evolving strategies used by criminals on the dark web.

The dark web marketplace offers a wide range of illicit products and services, allowing users to engage in anonymous transactions using bitcoin. According to a survey conducted by Privacy Affairs, there are several items available for purchase, including credit card information priced at $120, Russian passport scans priced at $100, stolen Facebook accounts priced at $45, and month-long DDoS attacks on websites priced at $850. Both individuals and organizations face significant risks when illegal services and confidential information are traded. Discovering one's personal information on the dark web is a significant matter that requires immediate action, such as contacting law enforcement. The need of implementing robust security measures and maintaining continual vigilance in response to cyber assaults cannot be emphasized enough, since attempts to retrieve lost data will not address the underlying security vulnerabilities.

Conclusion and Suggestion

India has substantial challenges in the realm of cybersecurity and law enforcement due to the presence of the dark web. When a country becomes a safe haven for illegal activities such as cyberattacks and drug trafficking, it endangers both its citizens and national security. To successfully address these attacks, it is essential to have a mix of enhanced technological capabilities, international cooperation, and rigorous enforcement of cybersecurity standards.

The browsers Onion and Tor, which enable users to access the dark web, should be subjected to stricter regulations and surveillance mechanisms. Limiting individuals' access to these technology might potentially decrease the ease with which they engage in illegal actions. Propose and enact a novel legislation specifically targeting criminal activities conducted on the dark web. Crimes like as cyberattacks, drug and human trafficking, and the sale of illegal items and services should all be included within the scope of this legislation. To effectively monitor activities on the dark web, it is important to use advanced surveillance technology. Enhancing cyber intelligence capabilities would facilitate the identification and apprehension of those involved in illegal transactions and activities.

Promote the dissemination of information on recommended cybersecurity procedures and enhance public awareness of these practices. To reduce the number of cybercrime victims, it is possible to implement public education programs that highlight the dangers of the dark web and provide advice on protecting personal information. Collaborate with international law enforcement agencies to combat illicit activities on the dark web by exchanging information and coordinating actions. Given the global nature of criminal activities on the dark web, it is essential to have coordinated international efforts. Establish an exclusive task force with the sole objective of combating illicit operations carried out on the dark web. In order to provide a comprehensive strategy to addressing these problems, it is imperative that this task group include experts in cybersecurity, law enforcement, and legal matters. Make a continuous investment in the research and development of cybersecurity. To stay ahead of cybercriminals, it is crucial to continuously develop and adapt to new strategies and threats.

Iraq, Turkmenistan, and Belarus have implemented stringent measures to crack down on VPN services in order to restrict illicit internet activities. These restrictions shed light on the global challenge of striking a balance between cybersecurity and individual privacy rights, potentially restricting online anonymity. Through an examination of these examples, India may enhance its regulatory framework to effectively balance the requirements of security and the significance of privacy in the contemporary digital age.