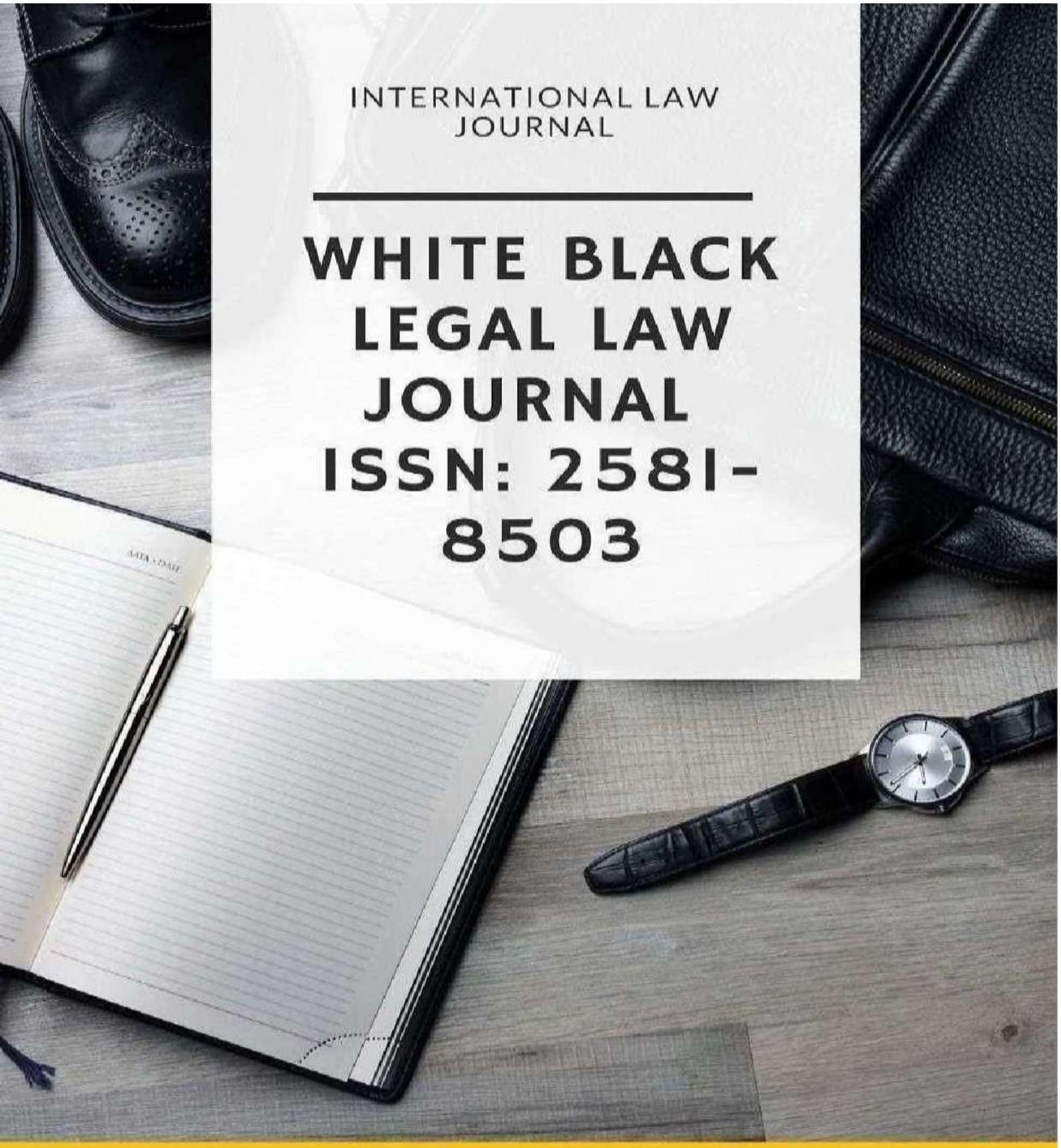

INTERNATIONAL LAW JOURNAL

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.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

DARKNET: ISSUES, CHALLENGES AND WAY FORWARD

AUTHORED BY - DIVYA ANN SAMUEL

Abstract:

The darknet presents a complex challenge as it stands at the intersection of privacy, cybersecurity and law enforcement. This concealed segment of the internet enables private communications beyond conventional surveillance. While it offers vital privacy protections, it facilitates illicit activities, like cybercrimes and data breaches, making it a complex task for law enforcement agencies, globally. The literature review reveals Lack of comprehensive strategies that effectively balance darknet regulation, privacy rights and cross-border law enforcement challenges, especially in Indian legal context. Thus, the research paper sets out to answer the research question on how can India effectively address the challenges of darknet-related crimes by balancing legal reforms, technological advancements and international cooperation, while protecting citizens' rights to privacy and free internet access. This paper argues that despite these challenges, a balanced and multi-dimensional legal framework grounded in Indian constitutional principles and complemented by international cooperation and technological innovation, would essentially combat darknet crimes. The study examines prominent data breach cases in India, the technological and jurisdictional hurdles in policing darknet and the legal landscape shaped by domestic and international efforts. It evaluates international legal instruments like Budapest Convention, to identify its limitation in addressing darknet crimes. Using the Silk Road case study, the paper highlights the ongoing struggle between darknet actors and authorities. The paper concludes by proposing a comprehensive strategy encompassing legal reforms, advanced technology, international collaboration and ethical enforcement.

Keywords: Darknet, Cybersecurity, Data Protection, Law Enforcement, Tor, International Cooperation

1. Introduction

Internet is an indispensable aspect of human lives so much so that its absence stands in direct loggerheads with fundamental rights. In the case of *Anuradha Bhasin vs. Union of India*[1], the hon'ble Supreme Court held that internet is a vital instrument for trade and business, especially for e-commerce operations as it provides a more accessible virtual marketplace, and, also, it acts as a platform for freedom of speech and expression. This makes it come under the ambit of Articles 19(1)(a) and (g) of the Constitution of India, which in turn implies that it can be restricted following a proportionality test under Articles 19(2) and (6). This aligns with the UN's emerging recognition of right to stay connected as a human right.[2] The State of Kerala became the first State to recognise access to internet as a basic human right.[3]

However, it is pertinent to mention that the searches that one gets at their clicks provide information from about 4% of the information available on the cyberspace.[4] This is akin to the tip of the iceberg metaphor. The internet space is divided in three layers: surface web, deep web and darknet. (Often, in common parlance, deep web and darknet are used interchangeably but the distinction between the two is stark and should not be overlooked.[5]) The webpages in surface web comprises of indexed pages that have been successfully identified by the search crawlers and have the quality of relatable content against users' search phrases.[6] If a webpage has no link, it can't be crawled into and would not appear in the search engine.

The deep web is that portion of the web that constitutes the maximum of web space and includes information protected by login or website database. This is the most sensitive information that mandates this privacy. For example, our email accounts, bank statements, direct messages on social media and photos shared in private, all come under this ambit.

Darknet goes deeper and is very aptly conveyed by its etymology. The uncertainty it carries is very apparent as not everything that runs on it can be known for sure. The brief history and the taxonomy of websites and activities that run on the darknet will be discussed in the next section. The paper will then move to address the mercurial nature of darknet because of its unknown facets from which fear and resistance germinates. Due to the apparent issues, there are various challenges that lurk for the law enforcement agencies (LEAs) all over the globe. However, after going through the scattered research endeavours by scholars from all fields, the researcher aims to culminate solutions that can concomitantly address the problem.

2. Darknet

The darknet is a specific part of hidden web where the key of operationality is the anonymity it ensures. "The darknet began with ARPANET, the Internet's progenitor, that was developed by the Pentagon in 1969. As the inter-computer interaction began to grow, a number of isolated, secretive networks started to appear alongside ARPANET. These networks eventually became the medium of choice for the US Naval Research Laboratory, which introduced a browser called TOR, which concealed the locations and IP addresses of users who download the software. However, the software became available for public in 2004."[7]

Search engines such as Tor, I2P and Freenet are used to access Darknet. The main application used for accessing darknet is The Onion Router (abbreviated as TOR) browser, where the onion metaphor indicates the layers of security that work to conceal a user's location, while providing access to websites with '.onion' suffix.[8] Tor has two main functions:

a) Create proxy servers for anonymity
b) Provide access to hidden networks.

"To operate effectively, the darknet has a small number of technological and infrastructure requirements, which are like those of legal content distribution networks. These infrastructure requirements are:

1. facilities for injecting new objects into the darknet (input)
2. a distribution network that carries copies of objects to users (transmission)
3. ubiquitous rendering devices, which allow users to consume objects (output)
4. a search mechanism to enable users to find objects (database)
5. storage that allows the darknet to retain objects for extended periods of time. Functionally, this is mostly a caching mechanism that reduces the load and exposure of nodes that inject objects."[9]

(See figure 1 for the infrastructural requirements of darknet)

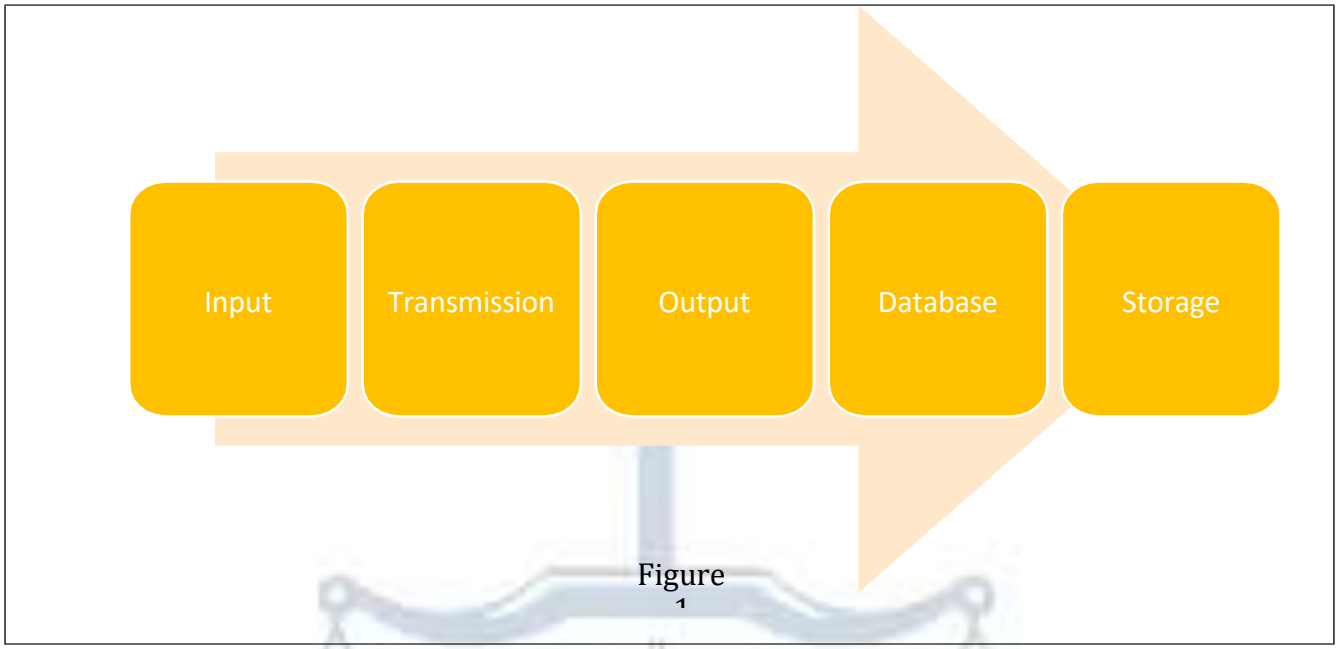

Figure 1

2.1 Activities on Darknet

The activities on the darknet are listed in the below:

Activism, journalism, and whistleblowing	**Criminal activities**	**Cyber security threats**
It is used by them to alarm governmental agencies about illegal activities such as slavery, child labour, child marriages, human trafficking, prostitution, and political dissents. "Secure Drop site is used by journalists and researchers for the anonymous communication and transfer of documents, promoting transparency about day-to- day issues and make the persons accountable. Some news channels use the deep web to stay secured from censorship. In 2019, BBC	People access darknet to access websites that sell drugs, weapons, and identities. It is also seen as a platform to hire assassins. These are the known goods and services on darknet. Silk Road was a portal to promote decentralisation of governments and socio-political movements against law enforcement agencies. Its ease of usage was akin to websites like	The tools used for hacking such as Malware, uses the Tor infrastructure to obtain the IP addresses of victims and record their keyboard strokes; while some malwares maintain secure communications between infected devices, and command server through the I2P hidden network.

created its own Tor website to provide access to their channels to bypass censorship by countries such as China, Vietnam, and Iran attempting to block their websites.'[10]	eBay.	

2.2 Effect of Darknet

The effect of darknet have been realised with positive as well as negative outcomes. The pros and cons of activities carried out over darknet are listed below:

Advantages	**Disadvantages**
Ensures privacy	Gateway to criminal activities "Some examples of dark web crimes: • Murder for hire: A site "Besa Mafia" used for contract killings. • Blackmail/ Extortion/ Ransomware Attack: Threatening people stating that they will disclose sensitive information or compromising photos till the victim pay the money.
	Illegal drug sales: AlphaBay, the largest dark web site was shut down in 2017 for selling fraudulent identification, counterfeit goods, malware, firearms, and toxic chemicals. Illegal arms sales: Guns were sold illegally without proper license on the dark web site. Terrorism: Many terrorist organizations use the dark web for recruiting and planning attacks. Child pornography: As the amendments and punishments against child pornography has increased, many users started using dark

	web." [11]
Helps create communication between closed groups or societies facing extreme censorship and outsiders. Academic study of Tor metrics demonstrated that 60 percent of Tor's use is for lawful purposes. Political censorship tops the list of why users download Tor for noncriminal purposes.[12]	Sale and purchase of personal data, for instance, an anonymity ensuring network would form part of illegal transactions involving documents related to credit cards and passports, or where private information such as email addresses, phones numbers are also disclosed.
Creates anonymity and secrecy. As noted in a US Supreme Court decision, *McIntyre v. Ohio Elections Commission*, "Anonymity is a shield from the tyranny of the majority.... It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation...at the hand of an intolerant society"[13]	Doxing basically involves taking people's personal information and spreading it as widely as possible.[14]
Useful for journalists and whistleblowers, for example, WikiLeaks allows whistle-blowers to anonymously upload classified information. Tor runs Tail, an encryption operating system that Edward Snowden had used.[15]	
Even Facebook launched a Tor hidden service to enable users to avoid surveillance and censorship.[16]	
By creating datasets for authorship verification and identification, some chatrooms involving children are closely	

monitored to avoid their exploitation.	
The military can track terrorist activities and use darknet to launch denial-of-service attacks, intercept, and block enemy communications.	

3. Issues

The Tor network and the cryptocurrency bitcoin are two innovative technologies that have enhanced user anonymity and untraceable financial transaction.[17] It, therefore, is almost impossible to enforce rules or close the gateway to Darknet bridges or relays because of lengthy and complicated processes.[18] When the Chinese government attempted to block access to Tor, Tor Project Inc. introduced secret entrance nodes to the Tor Network, called 'bridges', which are very difficult to block.[19]

With several users heavily relying and using Tor network, the communication system cannot be simply banned.[20] It, however, can be policed, i.e. closely monitored.[21] The asymmetric encryption used in the onion technology is also difficult to crack, which in turn makes policing difficult.[22] This will be discussed in the coming sections.

"On the darknet, the sale of illicit items supports organised crime, exacerbate poverty and food insecurity, and jeopardise public safety and health. Furthermore, disseminating false material on the darknet can exacerbate conflict, threaten peace and justice, and have a detrimental effect on public health and education outcomes. Thus, studying the darknet and how it affects human behaviour is essential to comprehending the difficulties and ramifications of accomplishing the SDG. Even though the use of darknet has increased significantly and may influence several SDGs, a more thorough examination of how it aligns with different SDGs is necessary."[23]

3.1 Criminal Activities

As discussed above, briefly, darknet has been seen as a hub of criminal activities.
Some of these are discussed in detail below.

Child Abuse

"In 2011, Europol, coordinating with 13 national governments, launched Operation Rescue. The concerted law enforcement action uncovered 670 suspects and led to 184 arrests on child abuse imagery-related charges (Europol 2011). In July 2014, the UK's National Crime Agency arrested some 650 people on various child abuse charges, ranging from the possession of images to the actual abuse of minors (BBC 2014a). In 2015, another 50 suspects were identified in Northern Ireland and 37 charges were laid (BBC 2015). These are just a few examples of the successful instances of law enforcement uncovering paedophilia rings in the recesses of the dark Web."[24]

Cyberwarfare: Asymmetrical Hybrid Warfare

"Current estimates place global cyber losses at $6 trillion by 2021, with expectations that this will increase further in the future. Cyber warfare and cybersecurity have become a "whole of society" challenge that requires a unified, elevated strategy and 180° approach to combat the morphing threat. As we examine today's cybersecurity environment, we are looking through the wrong end of the telescope. It is only in the context of AHW (Asymmetrical Hybrid Warfare) that we can begin to fully understand cybersecurity's critical role for successful defense, protection, and resolution. We have learned to treat cybersecurity first and foremost as a human problem and a senior leadership challenge, not solely an IT issue."[25]

It must also be emphasized that AHW strategy is rooted in Unrestricted Warfare or war without rules.[26] The solution lies in: DarkNet research and triangulation, active surveillance as adversaries increasingly exploits this platform[27]

IPR related challenges

"The idea of the darknet is based upon three assumptions:

1. Any widely distributed object will be available to a fraction of users in a form that permits copying.
2. Users will copy objects if it is possible and interesting to do so.
3. Users are connected by high-bandwidth channels."[28]

"Any content protection system will leak popular or interesting content into the darknet, because some fraction of users--possibly experts–will overcome any copy prevention mechanism or because the object will enter the darknet before copy protection occurs. We see the darknet having most direct bearing on mass-market consumer IP-goods. Goods sold to corporations are less threatened because corporations mostly try to stay legal, and will police their own

intranets for illicit activities. Additionally, the cost-per-bit, and the total size of the objects have a huge bearing on the competitiveness of today's darknets compared with legal trade. For example, today's peer-to-peer technologies provide excellent service quality for audio files, but users must be very determined or price-sensitive to download movies from a darknet, when the legal competition is a rental for a few dollars."[29]

Drugs

5 students in Mumbai students were busted while dealing with the purchase of drugs via the dark web, according to an article in the Indian Express. The 1,400 LSD dots that these five students purchased cost 70 lakhs.[30]

"In the 2014 World Drug Report, the rise of hidden, Dark Net drug markets was belatedly acknowledged. The Report set out that the variety of drugs available on the Dark Net appeared to be "diverse and growing" and this posed unique challenges for law enforcement. As outlined by Interpol in the September 2014 Internet Organised Crime Assessment (iOCTA), the relationship between customer and vendor in the hidden markets is purely transactional. Criminals in cyberspace do not need to be close to the crime scene, they might never even travel to the target country, their activities can be conducted transnationally and with minimum effort and risk by hiding their identity, the Assessment notes. By contrast, in the off-line world criminals normally need to be physically present at the crime scene and can typically only commit one offence at a time."[31]

"As outlined by Martin (2014),[32] illicit drugs have been bought and sold on the internet since it was first established. According to Markoff (2005)[33], cited in Martin, the first online ecommerce transaction was a 1971 marijuana exchange between students at Stanford University using the Arpanet accounts at the institution's Artificial Intelligence Laboratory and their counterparts at Massachusetts Institute of Technology. This underlines the 'dual use' challenge that the advent of the internet posed for the IDCR, with unstoppable and positive advances in global communications creating an enabling environment for illicit drug supply and use."[34]

3.2 Menaces created by use of darknet in India

The table 1 below shows instances of data breach over the darknet in India. This, in a way, highlights the struggles of a developing country in dealing with darknet activities and should be seen as a common issue with any developing democratic country trying to establish its global financial footing.

Menaces of darknet in India[35]
• Juspay data was breached in January 2021 wherein data of around 10 crore cardholders was sold on the dark web for an undisclosed amount. It involved sensitive information of customers like email ids and mobile numbers and card transaction. • Mobikwik data that included sensitive information of 3.5 million users were put up for sale on the dark web in March 2021. The information contained the KYC details, addresses, phone numbers, Aadhar card details, etc. of Mobikwik users in India. The Reserve Bank of India (RBI) asked the digital wallet firm to get a forensic audit done with the help of CERT-IN (Indian Computer Emergency Response Team) empanelled auditor. • Domino's India data breach in April 2021 involved sensitive information of around 18 crore orders released on the dark web for sale as a searchable database. Alon Gal, the CTO of Hudson Rock, a cybersecurity firm, posted on Twitter that this data was sold for around Rs 4.5 crore in bitcoins. • BigBasket data (from a November 2020 data breach confirmed by the company) was allegedly leaked on the dark web in April 2021. The data contained details of over 20 million customers such as their email addresses, names, birth dates, hashed passwords, and phone numbers. The size of the database leaked was around 3.25 GB. A hacker group known as ShinyHunters, put the data on the dark web for download.
Table 1

4. Challenges

With an estimated 2.5 million daily users, Tor is by far the most popular anonymous internet communication system.[36] What matters is not what the technology is, but how it is used and what the net effect turns out to be. Framed from this perspective, the focus of public debate should move away from demonizing the technology, or looking for quick technological fixes, toward the idea that, like every other aspect of human society, the dark Net needs to be policed.[37]

Because of Darknet's multilingual, mixed-style, and clandestine communication features, even with the privacy shield, the accessible discussions are insufficient to identify the source. The onion, i.e. layered, technology establishes a chain where each network node receives a message that has been encrypted using asymmetric encryption.[38] Another challenge with

respect to the dark web is that most dark web sites are active for a period of 200 days to a maximum period of 300 days. Some also last for a period of less than two months, making it even more tedious to track them.[39]

"Unlike those operated by banks and payment processors, the Bitcoin payment system is managed by a distributed network of computers all around the world rather than a single trusted party. This means that transfers made on the Bitcoin network may not be controlled or censored by any intermediary."[40]

Added to these challenges there are three pertinent hurdles towards tackling darknet. The first one being the legality associated with use of internet for ethical purposes. This leads to one suggesting that law enforcement agencies should block the known sites that pose potential harm to the human beings. However, the Silk Road case study will illustrate the second challenge of not being able to create a barrier from new and improved criminal sites from coming up anywhere else in the world, making it a vicious cycle of cat and mouse chase. The next hurdle is the lack of a global legal framework as many countries continue to show reluctance towards ratifying the Budapest Convention.

4.1 Legality

Having understood that the issue that lies with the unethical and immoral use of darknet, we need to understand that a lot of ethical research and whistle-blowing activities are carried out on the darknet. Like with every invention, there are positive uses as well as negative uses of the darknet and it has not been banded illegal in most democratic countries. Even in India, darknet is legal to use. This could be seen as another facet of darknet that the user's IP address remains unknown and figuring out the nation of origin of the user is difficult and tedious. In other words, the issue of the legality of access in India will not come up because it is impossible to determine from which nation a user is accessing the Dark Web due to the location's secrecy.[41]
Moreover, the right to access the internet is slowly being recognised as a basic human right. As pointed out in the beginning in the case of *Anuradha Bhasin vs. Union of India*[42], the hon'ble Supreme Court of India held that internet is a vital instrument for trade and business, and, also, acts as a platform for freedom of speech and expression. In *Maneka Gandhi vs. Union of India*[43], the Court held that "procedure which deals with the modalities of regulating, restricting or even rejecting a fundamental right falling within Article 21 has to be fair, not foolish, carefully designed to effectuate, not to subvert, the substantive right itself."

"The proportionality test as outlined by *K.S Puttaswamy vs. Union of India*[44], states that the restriction must be meet the following test:

1. A legislation must be passed to achieve a legitimate goal for it to violate fundamental rights
2. The justification for imposing the restrictions which curtail the rights such as measures should be based on rationality, backed by justifications which are in consonance with the objective of restriction
3. The restrictive steps taken should be applied to achieve reasonable state objective and not to only curtail the constitutional freedom
4. During the formulation of the policy, special diligence should be paid to ensure that the policy serves the legitimate objective
5. The State must ensure adequate and effective safeguards to protect fundamental rights."[45]

Considering this new march towards a better inclusive society, banning use of darknet for legitimate purposes would run ante human rights. (See Table 2 for list of countries that have recognised access to internet as a right) In case the right is restricted, the heavy burden of balancing the proportionality test listed above would be cumbersome for law enforcement agencies. A way around this dilemma could be criminalization of specific activities that clearly fall within the general ambit of an offence under various statutes. These activities would be held criminal irrespective of whether committed over the darknet or otherwise. (See Table 3 for the list of offences under Indian laws) For example, whoever deals with narcotic drugs outside India is subject to punishment under this Act, according to Section 24 of the Narcotics Drugs and Psychotropic Substances Act, 1985. Now, if someone were to engage in external drug dealing on the dark web, that would undoubtedly be unlawful no matter whether the dark web was legal but the behaviour was not.

Country	**Enactment/Judgement**
Estonia	In February 2000 under Telecommunications Act

Greece	Article 5A (added in 2001) of the Constitution gave people the right to participate in the information society and at the same time-imposed duty on the State to provide facilities for access to electronically transmitted information.
France	The Constitutional Council declared access to internet a fundamental human right
Finland	It is the first country that provided broadband as a legal right to its citizens
Costo Rico	In 2010 verdict, its Apex Court recognised access to internet as part of the fundamental human right under Article 33 of its Constitution
Spain	It provided access to internet as a right in 2009
Canada	Internet access was declared as a basic service in 2016.
India	The Supreme Court recognised it as a fundamental right in 2020.

Table 2

Criminalization of illegal activities on the darknet[47]

- Section 67(B)7 of the Information Technology Act, 2000 and Section 14 and 15 of the POCSO Act, 2012 both impose severe penalties for child pornography. These are the only parts that address the crimes of pornography involving children.
- In addition, the Indian Penal Code, 1860, defines the punishments for offences that are carried out against minor girls. According to Section 366(A), anyone found guilty of coercing, inducing, or seducing a minor girl to engage in sexual activity is subject to a 10 years prison sentence as well as a prospective fine.
- The Indian Penal Code's Sections 372 and 373 address the buying and selling of girls for prostitution. These types of illicit activity have been observed. They are included in the scope of human trafficking, either directly or indirectly. Trafficking in people is

forbidden.

- The dark web is used for a lot of criminal activities involving child pornography. If you are discovered encouraging such behaviour, you could find yourself in serious difficulty. In addition to child pornography, selling criminal materials is prohibited, as is purchasing weapons and drugs.

Table 3

4.2 Silk Road: Case Study

Silk Road rose to become one of the most popular sites on the darknet because of its ease of use which was akin to any ecommerce websites of the time, with the only distinction that it was used for all sorts of illegal activities. The website was a breeding ground for all sorts of illegal goods and services imaginable, like drugs, hire for kill, weapons, etc. The key advantage of Silk Road 1.0 over competitors was the site's use of Bitcoin digital coins which are not issued by any government, bank, or organization, and rely on cryptographic protocols and a distributed network of users to mint, store, and transfer.[48] Ross Ulbricht, the Dread Pirate Roberts (the moniker used by him at the time of creation of Silk Road), was arrested in October 2013 and the site was taken down. [49] This was, however, short-lived.

After Silk Road's interdiction, there was a rise in registration on other Dark Net sites such as Black Market Reloaded and Sheep Marketplace, which provided a mechanism for verifying trusted Silk Road vendors to encourage their customers to follow. Closing Silk Road and arresting Dread Pirate Roberts had no long term or catastrophic impact on the Silk Road project or hidden markets more broadly; quite the reverse. It stimulated new competition, innovation in business models and the launch of Silk Road 2.0 as communicated by Libertas one of the moderators on Silk Road in November 2013, just one month after the arrest of Ulbricht.[50]

"Again, the website expanded rapidly, quickly having as many as 150,000 active users and processing, according to FBI records, as much as $8 million in monthly sales. Blake Benthall, the Silk Road 2.0 site administrator and former Space-X employee, was arrested. Another win, another drop in the pond. Silk Road 3.0 was online within a few hours of Benthall's arrest." [51] Silk Road 2.0 was taken down under a mass operation called Onymous, in which representatives from the law enforcement agencies of 17 countries gathered at Europol to

collaborate on one of the biggest operations against dark-web websites.[52]

Silk Road's fall shows the limits of such a system, especially in the hands of negligent administrators. At the same time, the second wave of markets that has followed also shows that certain aspects of Silk Road's model worked exactly as intended.[53] This case study illustrates that there is no end to cropping up of new and improved websites on the darknet. It is the law of demand and supply. The more people go looking for niche services, the more vendors will find a way to reach them.

4.3 The Budapest Convention on Cybercrime 2001

One way to block websites like Silk Road could be to have global takedowns by law enforcement agencies. As cybercrimes have no jurisdictional boundaries, each country should share the burden of contributing to the global action plan to curtail illegal activities originating withing its territorial bounds. This could also imply sharing the necessary technology and information necessary. A concerted efforts from all the countries could prove beneficial. This is not a novel approach. In fact, there exists the 2001 Budapest Convention that calls on all the global powers to come together against cybercrimes.

"The Convention on Cybercrime aims to create a uniform legal framework for cybercrime and facilitate international cooperation in investigating and prosecuting such crimes. Cybercrimes are defined as those committed using a computer as either a tool or a target. The convention has been ratified or acceded to by 49 countries, including most members of the Council of Europe as well as non-members such as the United States. Article 6 of the Convention criminalizes the sale, procurement, import, and distribution of code and other hacking tools. Despite the existence of the convention, however, effective control over the Dark Net remains elusive."[54]

"In some countries, the treaty has come into force only recently, while some key European nations—Greece, Ireland, and Sweden—have yet to ratify it. While recognising that 'the impact of the Convention on Cybercrime cannot be measured solely by the number of States that have signed or ratified the Convention', the UN Office on Drugs and Crime noted in 2010 that 'compared to global standards, the number and speed of signature and ratification certainly remains an issue'…. A few important countries have not signed or ratified the convention, including countries with some of the highest cybercrime rates in the world, such as Russia,

China, India, and Brazil. This has led the CEO of Kaspersky Lab to describe the Budapest Convention as a 'convention of the victim countries'."[55]

Thus, the efforts to come up with a consensus for a common international convention has been proven futile and poses the biggest challenge in tackling the vices of darknet.

5. Way forward: Solutions

The issues and challenges discussed above make it plenty clear that there needs to be a proactive endeavour that needs to be taken at global scale. Having realised this, the law enforcement agencies across the world are working with coordinated ability to close down darknet marketplaces. "According to Bitcoin Magazine, the current shutdown of the dark website Wall Street Marketplace involved the concerted efforts of the German Federal Criminal Police, the Dutch National Police, Europol, Eurojust, and assorted U.S. government agencies, such as the FBI, IRS and DOJ."[56] (See Table 4 for some instances of successful takedowns of some darknet websites)

"There is evidence that the darknet will continue to exist and provide low cost, high-quality service to a large group of consumers. This means that in many markets, the darknet will be a competitor to legal commerce. From the point of view of economic theory, this has profound implications for business strategy: for example, increased security (e.g. stronger DRM systems) may act as a disincentive to legal commerce….This means that a vendor will probably make more money by selling unprotected objects than protected objects. In short, if you are competing with the darknet, you must compete on the darknet's own terms: that is convenience and low cost rather than additional security."[57] Based on this, the following solutions are proffered.

Computing solutions

"It is recommended that efforts be focused on three key areas. The first is the development and deployment of new technologies, such as cloud computing, to effectively combat the rapidly growing Dark Net. Second, there is a need to train and maintain skilled teams to leverage technology in the fight against cybercrime. Finally, building international partnerships is crucial given the lack of boundaries in cyberspace. By focusing on these areas, law enforcement agencies can enhance their ability to effectively combat cybercrime and maintain public safety."[58]

There have been attempts to create an automated operational system that would help detect and

notify users of new viruses or exploits in the darknet by integrating machine learning and artificial intelligence with an accuracy of more than 80%.[59] Some researchers have tried to integrate game theory into algorithms to generate specific policies based on user-vendor behaviour and such researches must be encouraged at the outset.[60] Scientists have effectively shown how to identify anomalous behaviours using a non-parametric HMM (Hidden Markov Model) and LDA (Latent Dirichlet Allocation) which helped them detect common discussion themes over the darknet.[61]

"There exist, however, many more successful techniques for bridge enumeration (Ling, Luo and Yang 2012) — that is, detecting potential bridges without asking the Tor Project for a list or scanning suspect servers. A simple approach is to run a Tor relay and monitor all of the circuits built through your relay. It is easy to identify whether you are the middle relay, so you can simply identify the previous hop and if it is not in the network it is probably a bridge. This technique is not foolproof because not all bridges will connect through your relay all of the time; hence, you must run many relays offering a significant proportion of the bandwidth to detect most of them, and even then, you will only detect most, but not all."[62]

Rules for data collection and storage

"With respect to the repeated data breach incidents, a specified regulation on the amount of personal data collection by various companies and their automatic deletion after a stipulated time period could increase the efficiency of cyber systems and secure the data and prevent such incidents in the future to a large extent."[63] 'The principle of privacy by design (or data protection by design as laid down in Article 25 of the GDPR) can be used to protect the rights of individuals that behave lawfully on the Dark Web. The principle entails that in the development of tools or services, the protection of privacy is embedded. This can be done by implementing techniques to secure the data, by anonymizing or pseudonymizing the data when possible, and by means of contracts and working instructions.'[64]

Collaboration with TOR Project Inc.

"Tor Project Inc. has supported many LEAs in the US and Europe by explaining how to use Tor for LEA (Law Enforcement Agencies) operations and how criminals may use it, as well as by developing tools and documentation that can assist LEA operations. However, they would not be willing to specifically advise LEAs on ways to exploit limitations in the Tor software. The Executive Director of Tor Project Inc., Andrew Lewman, says he would like to intensify collaborations with LEAs and policy makers in the UK."[65] LEAs in liberal democratic

jurisdictions should as far as possibly adopt a targeted approach to policing the Dark Web, focusing on exposing, disrupting, and prosecuting criminals while refraining from interfering with innocuous activities and the exercise of political freedoms.[66]

Policing

"The network is fragile, despite its resilience, and if we try to find a quick and easy technological fix to problems that are actually social, we run the very real risk of breaking the Internet. Rather than discarding Tor or breaking the anonymity and encryption of the system through back doors for law enforcement, the focus should instead be on policing what goes on upon the network itself. Policing has the advantage of minimizing the costs that the dark Web imposes on society, while allowing the dark Web to have the maximum potential positive effect globally."[67]

Policing here means a continuous monitoring of the darknet and taking down the websites that carry the potential to hamper the society, as was done in the case of Silk Road. The undying spirit to combat such menaces, despite their repeated popping up would require highly skilled professionals and adaptation by the law enforcement agencies.

Studying patterns for cryptocurrency

OSINT tools use techniques such as natural language processing and sentiment analysis to extract meaningful insights and patterns. They can even be used to track cryptocurrency transactions.[68]

Honeypot trap

Another well-known tactic that is often used by Law Enforcement Agencies is called the honeypot trap. Honeypot traps are cybersecurity techniques that involve setting up a system or service with the purpose of attracting and capturing criminals and malicious actors.[69]

Multilateral Treaties

There's potential for cross-border cooperation through the framework of the Budapest Convention, but better coordination at the international level should not be to the detriment of ensuring that national capabilities are sufficient to address the threat.[70] If need arise, more such multilateral treaties can be negotiated to gain traction in information sharing relating to the criminal activities on the darknet.

Successful Takedowns[71]

- As part of the Operation Paris (OpParis) campaign launched by the amorphous hacker collective, Anonymous, after the 2015 Paris attacks, hundreds of websites on the dark web associated with ISIS were taken down.
- A Russian citizen named Kirill Victorovich Firsov was imprisoned for 30 months for his role in selling stolen credit card information and other data on the dark web that was in turn used to execute other criminal activities, as per a US Department of Justice (DoJ) release on May 24 2021. Firsov was the administrator of a website that provided stolen personal information and other services.
- On June 11, 2021, the Tor-based market on the Dark Web called 'Slilpp' was shut down. Slilpp was responsible for dealing in stolen credentials on the dark web and offered its users access to as many as 1,400 websites, 80 million accounts and services worldwide.
- A Ukrainian national (extradited to the US in June 2019 after arrest in Spain a year earlier) linked to the cybercrime group FIN7 was sentenced to seven years imprisonment and ordered to pay $2.5 million. The group is responsible for stealing more than $1 billion from US citizens and organisations and selling them on the dark web.
- Ukrainian police announced on June 28, 2021 that advanced data analytics used by the Binance cryptocurrency exchange helped track down a group of money launderers called FANCYCAT, involved with numerous criminal scams, including laundering money for dark web operators and also the ‘Clop ransomware’ scam.
- A suspect involved in a series of cyber-frauds related to banks, telecom and multinational corporations was arrested by the Moroccan police on July 6, 2021, as part of Operation Lyrebird. The suspect attacked thousands of victims through phishing, credit card fraud and launched malware campaigns against the corporate networks of French-speaking communications companies.
- Data sites on the dark web associated with REvil gang became unreachable on July 13, 2021. It was speculated that this could be the result of prohibitions imposed by law enforcement agencies or the gang could have disbanded by itself. The REvil gang is the cybercriminal group that took credit for the massive international ransomware outbreak that happened on July 2 on the Kaseya IT management software.

Table 4

6. Conclusion

As pointed out above, there needs to be a dynamic mechanism to combat the menaces related to criminal activities on the darknet. This means a relentless concerted effort at a global scale by the law enforcement agencies (LEAs). Indeed, the criminal activities run on darknet are more talked about and elaborated everywhere but the underlying fact is that its uses cannot be outweighed. The goal of this research paper was to present the advantages and disadvantages of the darknet, and the spotlight on the criminal activities was shined only to proffer solutions. The solutions, suggested above, could start as a ballpoint mark for further studies and only when these are put to action can their viability be tested. As concluding remarks, Figure 2 highlights the takeaways from the above discussion.

Figure 2

Bibliography

1. United Nations, 'The Case for Connectivity, the New Human Right' (United Nations)
2. <https://www.un.org/en/un-chronicle/case-connectivity-new-human-right> accessed 25
3. April 2025.
4. Seema, 'Right to Internet: A Fundamental Right under Constitution of India' (2023) 3 International Journal of Civil law and Legal Research 44.
5. 'Dark Net - The Hidden Side Of Web' <https://informatics.nic.in/article/429> accessed

26 April 2025.

6. Masayuki Hatta, 'Deep Web, Dark Web, Dark Net: A Taxonomy of "Hidden" Internet' (2020) 19 Annals of Business Administrative Science 277.
7. InfoSec Newsletter Concept, 'Darkweb in a Nutshell'
8. <https://infosecawareness.in/newsletter/june21> accessed 26 April 2025.
9. Zakariye Mohamud Omar and Jamaluddin Ibrahim, 'An Overview of Darknet, Rise and Challenges and Its Assumptions' (2020) 8.
10. Peter Biddle and others, 'The Darknet and the Future of Content Distribution'
11. <https://www.cs.ucdavis.edu/~rogaway/classes/188/materials/darknet.pdf> accessed 26
12. April 2025.
13. Dr. G. Mala, 'Financial Crimes in Darknet: Challenges Faced by Law Enforcement' [2024]The Academic International Journal of Multidisciplinary Research 837.
14. 'Financial Crimes in Darknet: Challenges Faced by Law Enforcement' (n 10).
15. 'Darknet Master Tor and Deep Web Secrets (Procolo Scotto) 2020' < https://www.kufunda.net/publicdocs/Darknet%20Master%20Tor%20and%20Deep%20W eb%20Secrets%20(Procolo%20Scotto).pdf> accessed 27 April 2025.
16. Eric Jardine, 'The Dark Web Dilemma: Tor, Anonymity and Online Policing' [2015] SSRN Electronic Journal <https://www.ssrn.com/abstract=2667711> accessed 25 April 2025.
17. Mohd Akash, 'A legal analysis of the dark web: global and Indian perspectives' (2025) 5.
18. House of Parliament U.K, "The Darknet and Online Anonymity"
19. <https://researchbriefings.files.parliament.uk/documents/POST-PN-488/POST-PN-488.pdf> accessed 27 April 2025.
20. T. Casey Fleming, Eric L. Qualkenbush and Anthony M. Chapa, 'The Secret War Against the United States' (2017) 2 25.
21. Mohamed Thaver, 'The dark web and how police deal with it' (The Indian Express, 17 September 2018) <https://indianexpress.com/article/cities/mumbai/the-dark-web-and-
22. how-police-deal-with-it-5359482/> accessed 22 April 2025.
23. J. Martin (2014) Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs. London: Palgrave Macmillan.
24. J. Markoff (2006) What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry. London: Penguin Books.

25. Julia Buxton and Tim Bingham, 'The Rise and Challenge of Dark Net Drug Markets'
26. < https://www.swansea.ac.uk/media/The-Rise-and-Challenge-of-Dark-Net-Drug-Markets.pdf> accessed 27 April 2025.
27. Debopama Bhattacharya, 'The Dark Web and Regulatory Challenges'
28. <https://idsa.in/system/files/issuebrief/ib-the-dark-web-dbhattacharya.pdf> accessed 28
29. April 2025.
30. Andrea O'Sullivan, 'Ungoverened or Anti-Governance? How Bitcoin Threatens the Future of Western Institutions' (2018) 71 90.
31. Purbita Mazumdar, 'Is the Dark Web Illegal in India: A Comprehensive Study' (2022) 2.
32. Calum Jeffray and Tobias Feakin, 'Underground web The cybercrime challenge' [2015] Australian Strategic Policy Institute.
33. Wesley Lacson and Beata Jones, 'The 21St Century Darknet Market: Lessons From The Fall Of Silk Road' <https://zenodo.org/record/58521> accessed 10 April 2025.
34. Mostafa Soliman, "Layers of the Internet: The Challenge of the Dark Web and the Need for an International Legal Framework".
35. John Robertson and others, 'Darknet Mining and Game Theory for Enhanced Cyber Threat Intelligence' (2016) 1 95.
36. Gareth Owen and Nick Savage, 'The Tor Darknet'
37. <https://www.cigionline.org/static/documents/no20_0.pdf > accessed 28 April 2025.
38. Rob Rowlands, 'Policing the Dark Web: Ethical and Legal Issues', University of Warwick and TNO.
39. Hasan Saleh, 'Beneath the Surface: Exploring the Dark Web and Its Societal Impacts' [2023].

[1] 2020 SCC OnLine SC 25.
[2] United Nations, 'The Case for Connectivity, the New Human Right' (*United Nations*) <https://www.un.org/en/un-chronicle/case-connectivity-new-human-right> accessed 25 April 2025.
[3] Seema, 'Right to Internet: A Fundamental Right under Constitution of India' (2023) 3 International Journal of Civil law and Legal Research 44.
[4] 'Dark Net - The Hidden Side Of Web' <https://informatics.nic.in/article/429> accessed 26 April 2025.
[5] Masayuki Hatta, 'Deep Web, Dark Web, Dark Net: A Taxonomy of "Hidden" Internet' (2020) 19 Annals of Business Administrative Science 277.

[6] InfoSec Newsletter Concept, 'Darkweb in a Nutshell' <https://infosecawareness.in/newsletter/june21> accessed 26 April 2025.
[7] Zakariye Mohamud Omar and Jamaluddin Ibrahim, 'An Overview of Darknet, Rise and Challenges and Its Assumptions' (2020) 8.
[8] 'Dark Net - The Hidden Side Of Web' (n 4).
[9] Peter Biddle and others, 'The Darknet and the Future of Content Distribution' <https://www.cs.ucdavis.edu/~rogaway/classes/188/materials/darknet.pdf> accessed 26 April 2025.
[10] Dr. G. Mala, 'Financial Crimes in Darknet: Challenges Faced by Law Enforcement' [2024]The Academic International Journal of Multidisciplinary Research 837.
[11] 'Financial Crimes in Darknet: Challenges Faced by Law Enforcement' (n 10).
[12] 'Darknet Master Tor and Deep Web Secrets (Procolo Scotto) 2020' < https://www.kufunda.net/publicdocs/Darknet%20Master%20Tor%20and%20Deep%20Web%20Secrets%20(Procolo%20Scotto).pdf> accessed 27 April 2025.
[13] Eric Jardine, 'The Dark Web Dilemma: Tor, Anonymity and Online Policing' [2015] SSRN Electronic Journal <https://www.ssrn.com/abstract=2667711> accessed 25 April 2025.
[14] Jardine (n 13).
[15] Mohd Akash, 'A legal analysis of the dark web: global and Indian perspectives' (2025) 5.
[16] 'Dark Net - The Hidden Side of Web' (n 4).
[17] Akash (n 15).
[18] Akash (n 15).
[19] House of Parliament U.K, "The Darknet and Online Anonymity" <https://researchbriefings.files.parliament.uk/documents/POST-PN-488/POST-PN-488.pdf> accessed 27 April 2025.
[20] House of Parliament U.K, "The Darknet and Online Anonymity" (n 19).
[21] Jardine (n 13).
[22] Akash (n 15).
[23] Akash (n 15).
[24] Jardine (n 13).
[25] T. Casey Fleming, Eric L. Qualkenbush and Anthony M. Chapa, 'The Secret War Against the United States' (2017) 2 25.
[26] T. Casey Fleming, Eric L. Qualkenbush and Anthony M. Chapa (n 25).
[27] T. Casey Fleming, Eric L. Qualkenbush and Anthony M. Chapa (n 25).
[28] Biddle and others (n 9).
[29] Biddle and others (n 9).
[30] Mohamed Thaver, 'The dark web and how police deal with it' (The Indian Express, 17 September 2018) <https://indianexpress.com/article/cities/mumbai/the-dark-web-and-how-police-deal-with-it-5359482/> accessed 22 April 2025.
[31] Omar and Ibrahim (n 7).
[32] J. Martin (2014) Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs. London: Palgrave Macmillan.
[33] J. Markoff (2006) What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry. London: Penguin Books.
[34] Julia Buxton and Tim Bingham, 'The Rise and Challenge of Dark Net Drug Markets' < https://www.swansea.ac.uk/media/The-Rise-and-Challenge-of-Dark-Net-Drug-Markets.pdf> accessed 27 April 2025.
[35] Debopama Bhattacharya, 'The Dark Web and Regulatory Challenges' <https://idsa.in/system/files/issuebrief/ib-the-dark-web-dbhattacharya.pdf> accessed 28 April 2025.
[36] House of Parliament U.K, "The Darknet and Online Anonymity" (n 19).
[37] Jardine (n 13).
[38] Akash (n 15).
[39] Bhattacharya (n 35).
[40] Andrea O'Sullivan, 'Ungoverened or Anti-Governance? How Bitcoin Threatens the Future of Western Institutions' (2018) 71 90.
[41] Purbita Mazumdar, 'Is the Dark Web Illegal in India: A Comprehensive Study' (2022) 2.
[42] 2020 SCC OnLine SC 25.
[43] (1978) 1 SCC 248.
[44] (2018) 1 SCC 809.
[45] Seema (n 3).
[46] Seema (n 3).
[47] Mazumdar (n 41).

[48] Omar and Ibrahim (n 7).
[49] Jardine (n 13).
[50] Omar and Ibrahim (n 7).
[51] Jardine (n 13).
[52] Calum Jeffray and Tobias Feakin, 'Underground web The cybercrime challenge' [2015] Australian Strategic Policy Institute.
[53] Wesley Lacson and Beata Jones, 'The 21St Century Darknet Market: Lessons From The Fall Of Silk Road' <https://zenodo.org/record/58521> accessed 10 April 2025.
[54] 'Mostafa Soliman, "Layers of the Internet: The Challenge of the Dark Web and the Need for an International Legal Framework"'.
[55] Calum Jeffray and Tobias Feakin (n 52).
[56] 'Darknet Master Tor and Deep Web Secrets (Procolo Scotto) 2020' (n 12).
[57] Biddle and others (n 9).
[58] Mostafa Soliman (n 54).
[59] Akash (n 15).
[60] John Robertson and others, 'Darknet Mining and Game Theory for Enhanced Cyber Threat Intelligence' (2016) 1 95.
[61] Akash (n 15).
[62] Gareth Owen and Nick Savage, 'The Tor Darknet' <https://www.cigionline.org/static/documents/no20_0.pdf > accessed 28 April 2025.
[63] Bhattacharya (n 35).
[64] Rob Rowlands, 'Policing the Dark Web: Ethical and Legal Issues', University of Warwick and TNO.
[65] 'House of Parliament U.K, "The Darknet and Online Anonymity"' (n 19).
[66] Rowlands (n 64).
[67] Jardine (n 13).
[68] Hasan Saleh, 'Beneath the Surface: Exploring the Dark Web and Its Societal Impacts' [2023].
[69] Saleh (n 68).
[70] Calum Jeffray and Tobias Feakin (n 52).
[71] Bhattacharya (n 35).