VOLUME 3 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DARK WEB AND ITS LEGAL COMPLICATIONS

- Sahil Patel[1]

INTRODUCTION

The dark web has become a significant concern for authorities and law enforcement agencies in India. It is a hidden part of the internet that can only be accessed through specific software, and it offers a wide range of illegal goods and services to users who seek to remain anonymous. This makes it a haven for criminal activities such as drug and arms trafficking, child pornography, and cyber fraud.

Despite its growing presence in India, there still needs to be more stringent laws to control the use of the dark web and the sale of illegal goods and services. India has been slow to respond to this threat, and many believe that the current laws need to be revised and need to be updated tokeep up with the evolving nature of the dark web. Furthermore, even when laws do exist, the enforcement of these laws can be challenging, leading to a lack of deterrence for those who engage in illegal activities on thedark web.

To address these challenges, India needs to adopt a comprehensive legislative policy to track illegal activities on the dark web. This will involve more significant investment in law enforcement and the development of more robust Cyber security measures to protect individuals and businesses from online fraud and other types of criminal activities. Additionally, regulating access to the dark web in India may be necessary, which could involve banning VPN so creating a mandatory charge for VPN registration. Overall, it is clear that India urgently needs to take action to combat the legal complications posed by the dark web.

Definitions

The United States Department of Justice defines the Dark Web as "a collection of websites that exist on an encrypted network and cannot be found using traditional search engines or visited using traditional web browsers."

[1] Student at Amity University Raipur

The Federal Bureau of Investigation (FBI) defines the Dark Web as "a collection of websites that are publicly visible, but hide the IP addresses of the servers that run them."

The Cyber Crime Investigation Cell (CCIC) of Mumbai Police defines the Dark Web as "aportion of the internet that is intentionally hidden and inaccessible through standard web browsers and search engines, and used for illegal activities."

The Ministry of Home Affairs (MHA) in India has defined the Dark Web as "a part of the deep web that is not visible on regular search engines and requires special software, configurations, or authorization to access."

The Indian Computer Emergency Response Team(CERT-In) has defined the Dark Web as "an area of the internet that is not indexed by search engines and requires specialized software or configurations to access, and is often used for illegal purposes."

In a tweet, *former Indian Intelligence Bureau officer, Ajit Doval,* described the Dark Web as "a virtual world where cyber criminals indulge in illegal activities like drug trafficking, arms smuggling, and espionage."

From the abovementioned definitions, we can infer that the Dark Web is a hidden part of the internet that requires specialized software or configurations to access. While it's often associated with illegal activities such as drug trafficking, arms smuggling, and espionage that could pose national security risks, it's also used for legitimate purposes such as protecting the anonymity of journalists and activists. To regulate the Dark Web, it's essential to focus on specific illegal activities rather than condemning the entire platform. However, the anonymous nature of the Dark Web makes it attractive to criminals who may use it for illicit activities. Addressing these activities is crucial to combat cybercrime and maintaining a safe internet. This can be achieved through a multi-faceted approach that involves law enforcement efforts, international cooperation, and education and awareness programs. By understanding the nature of the Dark Web and working towards a comprehensive strategy, governments and organizations can promote a safer and more secure internet for everyone.

Significance

1. Anonymity and Privacy: One of the critical features of the dark web is its focus on anonymity. It enables users to conceal the identities, location, and online activities by using encryption tools like Tor (The Onion Router).This can be valuable for

individuals living in repressive regimes or those seeking privacy for legitimate reasons, such as journalists, activists, or whistleblowers.

2. Freedom of Expression: The dark web allows individuals to freely express their opinions, share information, and engage in discussions without fear of censorship or surveillance. This can foster alternative perspectives and support open dialogue in environments where such freedoms are limited.

   Access to Restricted Information: The dark web hosts a vast array of websites and forums that contain information not readily available on the surface web. Some of these resources may include academic papers, government documents, whistle blowing Platforms, or archives of historical significance. While some of this information may be valuable for research or journalistic purposes, it can include illegal or harmful content**.**

3. Illicit Activities: Unfortunately, the dark web is also associated with various illicit activities, including selling drugs, weapons, stolen data, hacking tools, counterfeit currencies, and other illegal goods and services. It has become a marketplace for criminal activities, leading to concerns over drug trafficking, human trafficking, cybercrime, and other illicit behavior.
4. Cyber security and Digital Threats: The dark web provides a breeding ground for cyber criminals, hackers, and other malicious actors who exploit its anonymity to launch cyber attacks, distribute malware, or engage in identity theft. Their activities can have far-reaching consequences, compromising individuals' personal information, financial systems, and national security.
5. Law Enforcement and Investigations: The dark web poses challenges for law enforcement agencies due to the difficulty of tracking illegal activities and identifying the individuals involved. However, authorities have tried to infiltrate and shut down criminal operations on the dark web, focusing on disrupting illegal market places and apprehending individuals involved in illicit activities.
6. Ethical and Legal Concerns: The dark web raises complex ethical and legal questions. Balancing the need for privacy and freedom of expression with the necessity to combat criminal activities poses ongoing challenges for governments, policymakers, and society.

It is important to note that while the dark web has both positive and negative aspects, most

internet users do not need to access it, as the surface web and legitimate online services cater to their everyday needs.

OVERVIEW OF THE DARK WEB

How the Dark Web Works

The concept of the Dark Web is often shrouded in mystery and has become synonymous with criminal activity, such as illegal drug trade, weapon sales, and human trafficking. However, it is essential to understand that the Dark Web is simply a portion of the internet not indexed by search engines and is only accessible through specific software, like Tor.

As mentioned earlier, Tor stands for The Onion Router, which uses complex systems to anonymize a user's actual IP address, making it difficult to track their online activity. This anonymity has become a double-edged sword because while it provides privacy and protection to whistle blowers, activists, and journalists, it also provides a platform for illegal activities.

Moreover, the Dark Web has become a hub for online market places, such as Silk Road and Alpha Bay, where people can buy and sell illegal products and services anonymously. Transactions on these market places are often carried out using cryptocurrency, such as Bitcoin, which is difficult to trace. Thus, the Dark Web has become a hotbed for cybercrime and poses a significant challenge to law enforcement agencies worldwide.

Technologies used to access the dark web

Browsing the dark web: You might believe that navigating the dark web is simple, given all the activity and the impression of a bustling market. It's not. When everyone is anonymous and a sizable portion of them are out to defraud others, the environment is as disorganized and chaotic as you would anticipate.

Using the Tor anonymizing browser is necessary to access the dark web. Your requests for web pages are routed through a network of proxy servers managed by thousands of volunteers worldwide using the Tor browser, which hides your IP address and prevents it from being tracked. Tor works like magic, but the experience it produces is erratic, unreliable, and painfully slow—just like the dark web itself.

However, for those prepared to put up with the discomfort, the dark web.

Dark Web search engine:

Even the best dark web search engines need help to keep up with the constantly changing environment. The experience makes me think back to late 1990s web searches.

Even one of the best search engines, Grams, produces repetitive and frequently irrelevant results.

Dark web websites: Dark web websites look like any other site, but there are significant differences. One is the naming structure. Instead of ending in.comor.co, dark web websites endin .onion. That's "a special-use top-level domain suffix designating ananonymous hidden service reachable via the Torn network," according to Wikipedia.

Browsers with the appropriate proxy can reach these sites, but others can't.

Dark web websites also use as crambled naming structure that creates URLs that are often impossible to remember. For example, a popular commerce site called Dream

The market goes by the unintelligible address of "eajwlvm3z2lcca76.onion."

Scammers create many dark websites and move around a lot to avoid the wrath of their victims. Even websites that have been in business for a year or longer may vanish overnight if the owners decide to cash out and leave with the escrow funds they hold on behalf of clients.

The ability of law enforcement to track down and prosecute the operators of websites that sell illegal goods and services is improving. The largest source of illicit goods on the dark web, Alpha Bay, was successfully brought down in the summer of 2017 by a group of cyber police from three different nations, causing tremors throughout the network. But many business people moved elsewhere.

According to Patrick Tiquet, director of security & architecture at Keeper Security and the group's resident DDoS expert, the Tor network is particularly susceptible to DDoS because of its anonymity. To avoid DDoS, he explained, "Sites are constantly changing addresses, which creates a very dynamic environment." Because of this, "The quality of search varies greatly, and much of the information needs to be updated.

Common Uses of the Dark Web

There are three main reasons why people may use the Dark Web:

Anonymization:

People may want to safeguard their online identity for a variety of reasons. In some cases, this is because they would face danger if their identity were revealed, as in nations

where the government disallows a free press or where the political restriction is practiced, for instance.

Others, including those who have experienced cyber stalking or are worried about the safety of online banking, might use it to lower their risk of becoming a victim of crime.

Tor is mainly used for people to browse the open web anonymously; a tiny percentage of its traffic relates to Hidden Services (below).

Accessing Hidden Services

A hidden service, also called a "onion service," is one where Tor protects both the user's and the website's anonymity. This means that the site's IP address cannot be determined, meaning its host, location, and content are hidden. Due to how frequently the website name ends, Hidden Services are sometimes called "onion addresses."

Tor is not a Hidden Service, but the sites it hosts are. Hidden Services can be used legitimately, for example, for whistle blowing or to all members of the public to share sensitive information, such as knowledge about crimes, without the risk of reprisals. However, it is generally believed that most Hidden Services contain illicit material. They often require registration (username, password etc.) and some have 'VIP' sections, accessible only by an invite from the administrators or through an application made by the member and approved by the administrator.

Illegal Activity

The Dark Web may be used by people wishing to carry out illegal activities online, such as selling weapons or drugs. These kinds of operations, and the websites offering them, are often referred to as Hidden Services(above).

LEGAL FRAME WORK FOR THE DARK WEB IN INDIA

International Legal Framework

A section of the internet that is purposefully concealed and challenging for the general public to access is referred to as the "dark web." It is frequently linked to criminal activity, including Selling illegal substances, weapons, stolen data, and hacking services. Most existing laws and agreements that address criminal activity regardless of the channel used,

Including the internet, make up the international legal framework for the dark web.

Cybercrime Conventions: Several international conventions provide a legal framework for addressing cybercrime, including activities carried out on the dark web. The primary conventions in this regard are:

The Council of Europe Convention on Cyber crime (also known as the Budapest Convention):

This treaty aims to harmonize national laws, improve investigative techniques, and promote international cooperation in combating cybercrime, including offenses related to the dark web. It provides a framework for criminalizing illegal activities, collecting electronic evidence, and facilitating collaboration among participating countries.

The United Nations Convention against Transnational Organized Crime: Although not

Specific to cybercrime, this convention addresses organized criminal activities that can extend to the dark web. It encourages international cooperation to prevent and combat organized crime, including trafficking, money laundering, and corruption, which can be facilitated through the dark web.

Mutual Legal Assistance: Mutual legal assistance treaties (MLATs) enable countries to request and provide assistance in legal matters, including investigations related to the dark web. Through MLATs, law enforcement agencies can exchange information, gather evidence, and cooperate on cross-border investigations. These agreements facilitate international cooperation to combat transnational crimes that extend to the dark web.

Collaboration between Law Enforcement Agencies: International law enforcement agencies, such as Interpol and Europol, collaborate to tackle cybercrime and related activities on the dark web. They share intelligence, coordinate operations, and support member countries in investigations. These organizations play a crucial role in fostering cooperation and assisting national authorities in addressing criminal activities on the dark web.

Financial Regulations: Financial regulations also play a role in combating illegal activities on the dark web. Governments and financial institutions implement measures to prevent money laundering, terrorist financing, and other financial crimes associated with the dark web. These regulations require financial institutions to implement stricter due diligence procedures and report suspicious transactions, helping to disrupt illicit financial flows.

It's important to note that the dark web operates in a complex and constantly evolving environment, presenting challenges to law enforcement agencies and the international legal

framework. Coordinated efforts at the national and international levels are required to address the illegal activities associated with the dark web effectively.

National Legal Framework

1. Cybercrime Laws: Most countries have laws covering cybercrime, which can apply to dark web activities. These laws typically address hacking, identity theft, fraud, illegal access to computer systems, and distribution of malicious software. Prosecution of individuals involved in dark web activities often falls under these existing cyber crime laws.
2. Drug Trafficking and Illegal Marketplaces: The dark web is infamous for its illegal marketplaces, where drugs, weapons, stolen data, and other illicit goods are bought and sold. Many countries have specific laws targeting drug trafficking and the sale of illegal substances, both online and offline. Law enforcement agencies often work to track and apprehend individuals involved in these activities on the dark web.
3. Money Laundering and Financial Crimes: Dark web market places rely on crypto currencies like Bitcoin for anonymous transactions. Laws related to money laundering, such as anti-money laundering (AML) and know-your-customer (KYC) regulations, may apply to transactions conducted on the dark web. Governments and financial institutions have been increasingly vigilant in monitoring and regulating crypto currency transactions to curb illegal activities.
4. Child Exploitation and Pornography: The dark web is also known for hosting websites involved in distributing child pornography and exploitation. Countries have strict laws against child exploitation and pornography, andlawenforcementagenciesoftencollaborateinternationallytoidentifyandprosecuteoffendersinvolvedinsuchactivitiesonthedarkweb.
5. Surveillance and Law Enforcement: Some countries have specific legislationgrantinglawenforcementagenciessurveillancepowerstomonitorandinvestigateactivitiesonthedarkweb.Theselawsoftenrequirejudicialauthorizationforsurveillanceandprotect privacy rights while allowing authorities to combat criminal activities.

It's important to note that the dark web operates across national boundaries, making it challenging for any country to regulate it fully. International cooperation among law enforcement agencies and intelligence communities is crucial in addressing the challenges posed by the dark web.

Please keep in mind that the legal framework for the dark web is subject to change, and specific laws may vary depending on the jurisdiction. It's always advisable to consult the rules and regulations of your country for the most accurate and up-to-date information.

Challenges In Regulating The Dark Web In India

Regulating the Dark Web presents several challenges in India, as in many other countries. The Dark Web refers to a part of the internet that is intentionally hidden and not accessible through standard search engines. It allows users to remain anonymous, which facilitates illegal activities such as drug trafficking, hacking, cybercrime, and the sale of counterfeit goods or stolen data. Here are some difficulties India faces when it comes to regulating the Dark Web:

Technical Expertise: Investigating and regulating the Dark Web requires specialized technical knowledge and tools. Law enforcement agencies need experts who can navigate the complex technical infrastructure of the Dark Web, including using advanced encryption techniques, Tor networks, and Crypto currencies. Building and maintaining this expertise can be a significant challenge.

1. **Global Nature:** The Dark Web operates globally, transcending national borders. This creates jurisdictional challenges for law enforcement agencies, as the servers hosting Dark Web content may be in different countries. Cooperation and coordination with international law enforcement agencies are crucial to address this issue effectively.
2. **Encrypted Communications:** Communication on the Dark Web is often conducted using encrypted messaging platforms, making it extremely difficult for authorities to intercept and monitor conversations. Encryption technologies make obtaining actionable intelligence or evidence against individuals involved in illegal activities challenging.

3. **Evolving Technologies:** The Dark Web continually evolves, with new tools, techniques, and marketplaces emerging to circumvent regulation. As soon as authorities identify and crack down on specific platforms or market places, new ones quickly appear, making it a perpetual challenge to stay ahead of illegal activities.
4. **Limited Resources:** Regulating the Dark Web requires significant resources, including funding, technical expertise, and training for law enforcement agencies. Allocating adequate resources to combat the various threats the Dark Web poses can be challenging for governments, particularly in developing countries like India.

   A multifaceted strategy is needed to address these issues, including bolstering law enforcement capacity, international cooperation, raising public awareness of cyber security issues, improving legislation, and investing in cutting-edge technologies for tracking and monitoring nefarious activity on the Dark Web.

LEGAL AND ETHICAL ISSUES OF DARK WEB IN INDIA

Thedarkwebhasbecomeaplatformforillegalactivitiessuchasdrugtrafficking,cybercrime,and human trafficking. Reports suggest that criminal groups in Delhi are using the anonymity of the dark web to carry out illegal activities like drug trafficking, weapons smuggling, and Money laundering. These groups use crypto currencies like Bitcoin to make anonymoustransactions,makingit difficultforlawenforcement agenciestotrack themdown.

To combat this trend, the Delhi Police have formed a unique team of the Cyber Cell to monitortheactivitiesofdarkwebsyndicates.Theteamisworkingwithotherlawenforcementagencie sto track down and apprehend those involved in these illegal activities. In recent months, the police have carried out successful operations against dark web syndicates, including a process where they arrested a group of individuals involved in selling drugs on the dark web.

Themodusoperandiofthesedarkwebsyndicatesinvolvesusing"ToR,"ananonymitynetworkthat hides the user's identity, and creating Bitcoin to escape the money trail. Transactions areusuallymadethroughcryptocurrencyafterdealersarecontactedthroughVPN(virtualprivatenet work).Thedarknetisusedtoillegallyroutedrugs,includinghash,opium,weed,ayurvedictabletscont aining opium, and others,to Western countries.

The syndicates lure customers through advertisements resembling a restaurant menu featured on Instagram, Telegram, and Skype for interaction. The anonymity of the dark webmakes itdifficultfor law enforcement agenciesto track down those involved in illegalactivities, and using cryptocurrencies makes it even harder to trace the transactions. Theriseofdark websyndicatesin Delhiisa significantconcern forlawenforcementagencies.

Drug Trafficking in India

In recent years, India has witnessed a surge in illegal drug trafficking through the dark web.Criminal groups in Delhi and other parts of the country use the anonymity of the darkweb and cryptocurrencies such as Bitcoin to carry out their activities, making it difficult forlawenforcementagenciesto track them down.

These syndicates are using the dark web to sell various drugs, including hard chemicaldrugs like LSD, MDMA, and marijuana, as well as traditional drugs like hash, opium, andweed. They are also using ayurvedic tablets containing opium-like Kamini Vidrawan Ras andBarshasa,among others.

These syndicates are also using the dark web to illegally route drugs to Westerncountries. They lure customers through advertisements resembling a restaurant menu and feature them on social media platforms like Instagram, Telegram, Skype, etc.

According to the Ministry of Home Affairs, the Narcotics Control Bureau (NCB) has detectedthe use of the darknet and cryptocurrency for drug trafficking in 38 cases over the past threeyears.A special task force dedicated to monitoring suspicious transactions related to drugs on the darknet and cryptocurrency has been established to address this issue.

TwolocaldistributorsfromMumbai,suspectedtobehighlyskilledindarknet-relatedcomputing, were arrested by Narcotics Control Bureau (NCB) officials for theirinvolvement in a darknet-based drug network. The NCB officials successfully busted the drug network and apprehended the twoaccused.

Weapon Trading in India

There have been reports of weapon trading through the dark web in India; it is essential tonote that it is illegal to buy or sell weapons online. The dark web provides an anonymousplatform for sellers to offer weapons without revealing their identities, and buyers can purchasethemwithout revealing theirown.

It is believed that some criminal groups and terrorist organizations may be using the dark webto acquire weapons for their activities. The dark web's anonymity makes it difficult forlawenforcementagenciesto trackdownthoseinvolved insuch activities.

Tocombatthis,theIndiangovernmenthastakenstepstomonitorthedarkwebandpreventtheillegal trade of weapons. The National Investigation Agency (NIA) has formed a special teamto investigate such cases and is working with other law enforcement agencies to track downand apprehendthoseinvolved.

According to researchers from Michigan State University, the Dark Web has emerged as asignificantmarketplaceforthetradeofweaponsamidtheongoingglobaldebateongunregulations. Using Tor, a Dark Web browser, the team investigated howfirearmsare anonymously bought and soldacrossthe world.

The researchers found that 64% of the advertised products on the Dark Web were handguns,whilesemi-automaticlonggunsaccountedfor17%oftheproducts.Fullyautomaticlonggunsmadeup 4%of theproductsbeing traded.

According to officials from the Narcotics Control Bureau (NCB), the use of darknet andcryptocurrency for drug trafficking has been noticed in 38 cases in the last three years. A special task force on the darknet and cryptocurrency has been constituted to monitor suspicious transactions related to drugs on the darknet. Recently, the NCB busted a darknet-baseddrug network and arrested two local distributors from Mumbai who were believed to be well-qualifiedand experts in darknet-relatedcomputing.

HumanTraffickinginIndia

Human trafficking is a heinous crime that exploits vulnerable people for sexual or laborpurposes. Unfortunately, the dark web has become a hub for human trafficking in India.Criminal syndicates use the anonymity the dark web provides to traffic and sell humans,makingit difficult forlawenforcement agencies totrackthem down.

Approximately one-third of human trafficking victims are children, making them a significanttarget for traffickers. The dark web has become a thriving market for child trafficking, with manycasesreported.

Money Laundering in India

Money laundering is concealing the origins of illegally obtained money bytransferring it through legitimate businesses or financial institutions. Criminals engage inmoney laundering to make their illegal proceeds appear legitimate and avoid detection byauthorities. Using the dark web and cryptocurrencies makes it easier for criminals tolaundermoneyasitprovidesanonymityandmakesitdifficultforauthoritiestotracetransactions.

A private-sector bank in India partnered with a local payment gateway to selldownloadable software to customers in India. The merchant selling the software was basedoutsidethecountryandhadbeenvettedbythebankforlegitimacy.However,thiscase Highlights the potential for money laundering through such partnerships and transactions,particularlywith the riseof Chineseloan apps operatingin India.

Cyber Crime in India

Nuh, a district in Mewat located near Delhi, has been known for poverty, illiteracy, andoccasional crime like cattle smuggling. But now, it has become a hub for cyber crimes, withcriminals from Nuh victimizing people across India. Recent arrests have uncovered 28,000cyber crime cases in the country, and police from far-off places must come to Nuh to arrestscammers. The district's proximity to affluent cities like Delhi also makes it an easy target forcybercriminals to find victims.

CASE STUDIES AND LAW ENFORCEMENT IN INDIA

Case study of Dark web Activity

Around 5 million internet users' stolen data is being sold online,, and 600,000 are fromIndia, making India the worst affected country. The stolen data includes user logins, cookies,digital fingerprints, screenshots, and other information. The average price for a person's digitalidentityis$5.95,whichisaroundRs.490.ThisinformationcomesfromNord VPN,oneofthebiggestVPNserviceprovidersintheworld.BrazilandtheUSaretheothertwomostaffectedcountries.

Judicial Pronouncements

- *State of Maharashtra v. Saquib Nachan & Ors.*: In this case, the accused were foundtobemembersofaterroristorganization andwereusingthedarkwebto communicate and plan their activities. The court held that using the dark web for terroristactivitiesconstitutesanoffenseundertheUnlawfulActivities(Prevention)Act, 1967.

- *Sushmita Sinha v. Union of India*: This case dealt with the issue of the use ofcryptocurrency for illegal activities, including on the dark web. The court held thatcryptocurrency transactions fall under the definition of "electronic records" and can beusedasevidence.
- *R.v.MatthewDavidGraham*:ThiscasedealtwiththesaleofdrugsonthedarkWeb.The court held that the accused's actions amounted to drug trafficking under theNarcotic Drugsand Psychotropic SubstancesAct1985.
- *SatishK.S.v.StateofKerala*:ThiscasedealtwithusingthedarkwebtodistributechildPornography. The court held that using the dark web for such activitiesconstitutes an offense under the Information Technology Act, 2000, and the ProtectionofChildren from SexualOffencesAct, 2012.
- *StateofKeralav.MuhammadAshraf*Inthiscase,theaccusedwasfoundtobeusingthedarkwebtopurchaseandselldrugs.ThecourtheldthatusingthedarkwebfordrugtraffickingisillegalundertheнarcoticDrugsand PsychotropicSubstancesAct1985.

Agenciesinvestigatingcybercrimethroughthe dark web

I. *The Narcotics Control Bureau (NCB)* has been investigating the use of the dark weband cryptocurrency for drug trafficking and has set up a special task force to monitorsuspicioustransactions related to drugs onthe darknet.

II. *TheCentralBureauofInvestigation(CBI)*hasbeeninvestigatingcasesrelatedtoillegalactivities on the dark web, such as online fraud and hacking. In one case, the CBIarrested individuals for allegedly stealing data from a financial institutionandusing it to commitfraud.

III. *The National Investigation Agency (NIA)* has also been investigating cases related toillegal activities on the dark web, such as terrorism and arms trafficking. In one case,the NIA arrested an individual for allegedly using the dark web to purchase weaponsandexplosives.

IV. *TheCyberCrimePolice*ofvariousstatesinIndiahavebeeninvestigatingcasesrelatedto cybercrime on the dark web, such as phishing scams and identity theft. In one case,theCyberCrimePolicearrestedindividualsforallegedlyrunningaphishingscamon thedarkweb.

V. TheIndiangovernmenthasbeenstrengtheningitscapabilitiestoinvestigateillegal activities on the dark web, such as setting up a dedicated cyber crime

divisionwithintheMinistryofHomeAffairs.

Challenges in Investigating the dark web

The criminal underworld of the dark web usestechnologies suchas anonymization and cryptocurrency to conceal its dealings in various illicit goods, including drugs, weapons, childpornography,andevencriminalservicesforhire.Theanonymityprovidedbythedarkwebenables these illegal activities to thrive andmakesitchallengingforlawenforcementagenciesto detect and prevent them.

Despite the widespread impact of online crimes on their jurisdictions, many law enforcementagenciesremainlargelyunawareofthedarkweb'sexistenceduetoitsanonymity.Thispresents a significant challenge for authorities investigating and combating illegal activities on the dark web.

There are specific challenges faced while investigation.

1). Anonymity: the dark web use technologies like tor to conceal information relevant to theindividualsandorganizationscommittingcrime.Thismakesitdifficultforlawenforcementagencies totrack downtheindividualsand organizationsbehind theillegal activities.

2). Encryption: many dark web marketplaces use encryption to secure theircommunications and transactions. This makes it hard for law enforcement agencies to crack, decode the messages, and gather evidence.

3). Crypto currency: Dark web transactions generally use crypto currencies like bitcoin for transaction, which is difficult to trace; this makes it hard to follow the money train and catch the people behind illegal activities.

4). International jurisdiction: the accessibility of the dark web covers the whole world; anyone anywhere can use the dark web; this creates difficulty for law enforcement agencies to identify which country's law would apply to a particular activity, and this can develop jurisdictional challenges and hamper the ability of agencies.

5). Sophisticated techniques: Criminals on the dark web often use sophisticated methodslikesocialengineeringandmalwaretodeceiveandcompromiseindividualsandorganizations.Thismakesitdifficultforinvestigatorstoidentifyandtracethecriminalsresponsiblefortheseattac

ks.

Strategies for Combatting

It is a well-known fact that India's laws are not very stringent, and even the laws that do exist need to be enforced more effectively. To combat illegal activities, a comprehensive legislative policy must be adopted to keep track of them. Though it may not be easy to control citizens' activities, Indiacan limit its citizens' access to the dark web.

Indiahasmuchworktodotocontrolitscitizens'activitieseffectively.Currently,therearenospecificlawsinIndiatoregulatetheuseofVPNs.Somecountries,suchasIraq,Turkmenistan,andBelarus,haveentirelybannedVPNservices,whileothers,likeUAE,Russia,andChina,have restricted access to VPN services. These countries have either limited VPN usage to approved organizations or imposed strict regulations. India could also consider implementing such a system to ban freely available VPNs.

CONCLUSION

In conclusion, the dark web significantly threatens the safety and security of individuals,businesses, and governments worldwide. India is not immune to these threats, and its lawenforcement agencies face multiple challenges in investigating illegal activities on the darkweb. While India has laws in place to regulate online activities, they need to be strengthened,andtheirenforcement needs tobeimproved to tackle themenaceof thedark web.

Itisalsonecessarytorecognizethattheanonymityprovidedbythedarkwebisoneofthecriticalfactors enabling illegal activities to thrive. Therefore, implementing stricter regulations onaccess to the dark web by its citizens and banning freely available VPNs could help preventaccess to illegal activities. Additionally, developing better technology to track down criminalson the darkweb andcollaborating with international agencies to share information andexpertisecan help improveIndia'sabilityto combat cybercrime.

In conclusion, addressing the challenges the dark web poses requires a comprehensive approach involvingstrongerlaws,betterenforcement,improvedtechnology,andinternational cooperation. By adopting such measures, India can protect its citizens from thedangersofthedarkwebandsafeguard itsnational securityand economicinterests.