The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 2 | Issue 12 | December 2024
ISSN: 2583-973X (Online)
Website: www.theacademic.in

Financial Crimes in Darknet: Challenges Faced by Law Enforcement

Dr. G. Mala
Head and Assistant professor, Department of Criminology
JHA Agarsen College
Mala.gandhi02@gmail.com

ARTICLE DETAILS

Research Paper

Keywords:
Financial crimes, Darknet, Special browser, anonymity and Privacy.

ABSTRACT

Financial crimes are increasing day by day as everyone started using electronic gadgets for financial transaction. Generally, people use the visible part of the internet for the online transaction, but some few people use the deeper part of the internet called the dark net for the financial transaction to maintain privacy and anonymity. Many use the dark net for legal purpose, some use it for the illegal activities to secure their identities and stay safe from law enforcement. This paper attempts to identity the crimes in dark web and challenges faced by Law enforcement in identification, detection and prevent such crimes in dark web.

INTRODUCTION

Victims of financial crimes are increasing as the usage of modern gadgets for financial transactions are increasing. There are various reasons for the increase of these crimes. Identification, detection of these crimes are real challenge for the law enforcement as they need special skills. In addition to this, delays in the investigation process of these crimes are next important reason for the increase of these crimes. Ineffective Laws and implementation mechanism is another reason. Punishment is of civil nature. As normal offline crimes itself a tough task for police, internet crimes are still more difficult for law enforcement. As a result, Rich becomes more Richer and poor becomes poorer. These crimes have a profound impact on the society as the flow of money is not even.

Dark net is a platform to access internet safe and secure, but this feature is misused by cyber criminals. Recent Leakage of NET question paper via Darknet for INR 6 lakhs, is one such criminal activity. Therefore, this paper attempts to explore the issues and preventive measures taken by the law enforcement to curb the crimes in Dark net (part of internet)

DARKNET

The visible part of the internet is referred as surface web and used by ordinary users. The hidden part of the internet which is accessible by specialized tools is the deep web and not located through internet search engines. Usage of deep web is legitimate and legal.

HISTORY AND DEVELOPMENT OF DARK WEB

The US Department of Defence developed a network to protect the leakage of sensitive communications, which is not accessible to ordinary internet surfers. But the researchers, found it as a solution to maintain anonymity and privacy for the internet users. The private network originally used by defence department has become a public network.

SPECIAL BROWSERS FOR ANONYMITY THROUGH ENCRPTION

The Darknet cannot be accessed by normal browser, it needs a special browser. The following are some of the browsers.

TOR Browser: TOR (short for The Onion Router) created by the US Department of Defence to hide the user' details.

I2P Browser: One to one network to share confidential information, an alternative to TOR.

TailsOS: A Linux distribution which can be started from any storage device.

Orbot: For Android smartphones.

Tox: Tox is a free and open-source, end-to-end encrypted instant messaging and video calling application used to message and chat with friends in a secure manner.

IprediaOS: Developed for Linux platform for one-to-one communication, to send e-mails, to transfer files through the internet anonymously.

DARK WEB AND LEGAL PURPOSE:

As many as 65,000 unique URLs ending with. onion available on the Tor. In 2018, computer security firm Hyperion Gray in their study found that these networks are legal and used to provide communication via forums, chat rooms as well as E-commerce. In 2016, another organisation, Terbium Labs with 400. onion sites found that half of the sites in the dark web are legal.

USERS OF DARKWEB

According to the Statistics, more than 50% content on the dark web is of government organizations and private organisations such as Facebook and used for legal purpose. Only, few sites in the dark net used for drugs trafficking , fraud and hacking.

- **Legal users**

- Whistle-blowers can meet the public online to discuss the functioning of the government and change opinion, bring sensitive and secret information of political and powerful personalities to light and make the government accountable for their wrong doings. Whistle blowers should not be at risks as they accuse persons and organisation in power for their wrong deeds and secure them from chances of getting imprisoned. Darknet, provide a secure communication platform as it maintains user anonymity.

- **SecureDrop** site 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 secure from censorship. In 2019, BBC 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.

- Governments do use the dark web, primarily for intelligence gathering and to monitor criminal activity, also potentially using it for secure communication in sensitive situations where privacy is crucial; however, accessing the dark web does not automatically imply illegal activity by a government agency.

- Law enforcement: Law enforcement officials like normal internet users access the dark net for undercover operation and part of surveillance to catch criminals. As dark net is anonymous, others not able to find out who is there in the opposite side.
- Cybersecurity researchers

- Censorship issues: Some countries block the internet access or some sites to prevent access to news channels. In those countries, people use the dark net to access news channels anonymously to prevent action from their government.

- People might seek medical advice through online mode confidentially. Dark net is the right platform for such kind of people.

➢ **Illegal uses**

Though, dark web is used for legal and genuine purpose, cyber crooks and notorious users use it for many illegal activities as it provides a shield from not getting caught.

Example

- Trafficking and selling of drugs, weapons and Human.
- Hacking passwords, and steal identities of others (Identity theft)
- Distributing obscene materials (pornography) and other harmful materials
- White collar crimes like Money laundering and cyber crimes
- Selling pirated softwares and malwares by cybercriminals to steal personal data for financial gain.

REASON FOR INCREASE OF ILLEGAL & CRIMINAL USAGE IN DARKWEB:

Generally, internet does not provide privacy and anonymity, anyone can track us, and therefore a special service is needed to maintain confidentiality.

One of the best features that the dark web provides is "ANONYMITY AND PRIVACY" and useful for right people for good purpose. Like a coin as two side, the same service is misused by notorious criminals for illegal criminal activities. Privacy networks use multiple layers of complex encryption and random routing to hide the user's details. The anonymity the dark web provides is the cause for increase of black markets, drug deals, and cyberattacks.

PAYMENT METHODS

Normal payment uses bank transaction, where easy to predict sender and the receiver. But the payment in dark web is made using crypto currency. The way payments are processed adds another layer of anonymity.

Most of the financial transactions in dark web is done through cryptocurrencies. This provides another layer of privacy and difficult to identity the user and also reduces the chance of getting caught by law enforcement agency, has led to expectations of a boom in crime. A cryptography expert Satoshi Nakamoto created the world's first cryptocurrency using cryptographic algorithms and named it as "Bitcoin" and uses decentralised network which is not controlled by a national government. Cyber criminals started to use Bitcoin cryptocurrency for illegal transactions on a dark-web site. Silk Road, a dark web site, only accepted payment via bitcoin. In general, use of bitcoin or use of bitcoin in dark web is not illegal. Use of bitcoin for illegal activities and transactions is the real issue and challenge for the law enforcement officials. This is another reason for the increase of criminal activities in Dark web.

TYPES OF ILLEGAL CRIMINAL ACTIVITES AND CYBER SECURITY THREATS IN DARK WEB & CASES INVESTIGATED BY POLICE

Terbium Labs an organisation found out from a sample of 200 dark web sites, more than 75 percent sites used for illegal activities for selling Recreational and pharmaceutical drugs, credit cards and bank credentials, pornography and counterfeit goods.

In 2013, the Federal Bureau of Investigation (FBI) arrested Ross Ulbricht for illicit drugs.

Crimes with covert transactions were often committed through the dark web to protect the identity of the criminals.

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.

A recent report by a leading crypto-payment analytic firm, Chainalysis, shows that Bitcoin transactions on the dark web grew from approximately $250 million in 2012 to $872 million in 2018. The firm projected that Bitcoin transactions on the dark web will reach more than $1 billion in 2019. Even though the total economic volume of illicit dark web activity remains relatively small, many of the most corrosive threats to society today operate in the shadows of the Tor network and thus attract the attention of international regulators, financial institutions, and law enforcement agencies.

INVESTIGATION TECHNIQUES AND CHALLENGES FACED BY LAW ENFORCEMENT

Undercover : Law enforcement officers imitate as sellers to obtain buyer's mailing address.

Shipping procedures provide investigators with valuable information. Finally, the products ordered through dark web reaches the destination. Law enforcement can get the aid of postal service to trace the criminals.

Surveillance Law enforcement agencies can use surveillance footage, handwriting analysis, and Fingerprints on packages to trace the sender's identity.

Special Law enforcement: special police officers to track cybercriminals may speed up the investigation.

Hacking techniques: Use of hacking techniques and planting malware to track the IP Address. Exploiting the vulnerability in the browser, allowing investigators to see the IP addresses of dark web marketplaces and users.

MEASURES TAKEN BY LAW ENFORCEMENT AND LEGISLATORS TO CONTROL CRIMES

- **Interpol and Europol**

Interpol and the European Union obtain intelligence from dark net and shared with Law enforcement. Nearly 50 illicit dark-web sites were shut down.

- **Financial Action Task Force**: Financial Action Task Force was started in June 2019 to collect cryptocurrency transaction details to identify both the sender and receiver.

- **INFORMATION TECHNOLOGY ACT, 2000** : IT ACT was amended in the year 2008 and again in 2021 to tackle various cybercrimes.

- **CCISOM** is a Project aims to address the illegal use of new technologies.

CONCLUSION

Accessing Darknet and using cryptocurrencies for the transaction does not constitute crime. The purpose for which it is used is the real issue and challenge for the law enforcement. Therefore, government need to conduct surveillance and gather intelligence to apprehend the cyber criminals and to create a safe and crime free society. Strict and stringent laws with imprisonment along with fine can only control these crimes.

REFERENCES

- Shubhdeep Kaur, Sukhchandan Randhawa. (June 2020). Dark Web: A Web of Crimes. Wireless Personal Communications, 112(4). Pages 2131 – 2158 https://doi.org/10.1007/s11277-020-07143-2.
- Ryan Mason & Galen Flanigan. (March 2024). Journalism Targeting on the darkweb. https://tech4humanitylab.org/blog/2024/3/10/journalism-targeting-on-the-dark-web.
- Project CCISOM: new technologies. Cyber challenges in smuggling of migrants and human trafficking. (2022-2024). https://www.interpol.int/en/Crimes/Human-trafficking-and-migrant-smuggling/Project-CCISOM-new-technologies.
- Tanya Aggarwal. (Sep 2024). The dark web demystified: Its role in privacy, crime, and regulation. https://www.orfonline.org/expert-speak/the-dark-web-demystified-its-role-in-privacy-crime-and-regulation.
- Adarsh Tripathi. (Jul 2024). Unveiling Shadows: Exploring the Dark Web's Impact on Indian Law and Society. https://articles.manupatra.com/article-details/Unveiling-Shadows-Exploring-the-Dark-Web-s-Impact-on-Indian-Law-and-Society.