THE DIGITAL UNDERWORLD: MODERN EAR OF CRIME THROUGH THE DARK WEB

Radhika Garg[*] Yash Bansal[*]

ABSTRACT

*As we all know technology changes day by day and it makes our life easy because of the net and develop digital technology. But all things contain more than 1 face because the developing technology contains some different ways of a crime other than useful ways. One of its dark sides refers in this paper is the **"DARK WEB".** This article contains drew attention to digital crime through the dark web, in addition to highlighting various aspects of crime through the dark web including cryptocurrency. How to make access through the dark web, the dark web was successfully takedown by the government, tor in a nutshell. It also contains Statistics on the dark web in India and related laws to regulate dark web crime.*

Keywords*:* Dark Web, Digital, Network, Cyber Ethics, Crypto, TOR Browser.

INTRODUCTION

The most popular web browsers can be applied to instruct well-known web search engines to find a huge percentage of the content that is present on the World Wide Web. These search engines provide the Uniform Resource Locator (URL) addresses of websites so that users can quickly find them and connect to them using their web browsers. Moreover, there is also content on internet-connected computers (also known as servers) which can be found or indexed by normal search engines; access to these materials frequently necessitates a straightforward Web location and perhaps IP (Internet Protocol) address, as well as a passcode or other security measures. In other words, users have to prepare in advance to access this stuff.

Without special equipment or setups, one cannot access the network of sites known as the "dark web." General search engines don't index it. It frequently has connections to unlawful transactions such as drug, trafficking, the sale of firearms, and other crimes. Furthermore, it provides markets, forums, and anonymous social networks where users may communicate

[*] BCOM LLB, SECOND YEAR, GLA UNIVERSITY, MATHURA.
[*] BTECH, SECOND YEAR, GLA UNIVERSITY, MATHURA.

and share information. The dark web has evolved into another haven for activists, cybercriminals, and other people who seek to conceal their identities and dodge repression because of its anonymity. The dark web is a hazardous place where criminals and predators operate, despite the fact that it may be a useful resource for privacy and free speech. When utilizing the dark web, it's crucial to be wise and cautious.

Only a special web browser known as a "Tor network" (the onion router) may access a section of the internet known as the "dark web" Other names for the darknet or the unregulated internet **Crime through the Dark Web Including Cryptocurrency**

A general definition of the darknet is a covert (or anonymous) communication system that is secret, encrypted, and both. Ordinary Internet users typically cannot access or see such a covert communication route. The Onion Browser (Tor) networks and the black web are both connected to the darknet. The primary goal is to protect the privacy of user activity.TOR can be used to offer anonymous access to already-existing websites.[1] The covert character of The Tor network's onion websites can be used to enable a variety of illegal services, including the Silk Road marketplace, where anonymous payment methods, such as bitcoins,[2] are frequently employed. The many dangerous cyber operations which are reported to be carried out on the dark web and made possible by cryptocurrency will now be quickly reviewed.[3]

Cryptocurrencies such as Bitcoin and ransomware A form of malicious software known as ransomware threatens users by restricting access to their private data until a ransom is paid (usually with some sort of cryptocurrency).[4] In actuality, physical kidnapping, and cryptocurrencies were also used as payment.[5] As per the global cyber defense annual report published on July 2021,[6] 304 million ransomware intrusions were reported globally in the year 2020, which was a 62 percent increase from 2019 as well as the second-greatest rate since 2016. It has the greatest infection rate in recorded history and has caused at least $4 billion in harm worldwide across 150 countries.

[1] Janis Dalins, Campbell Wilson, and Mark Carman. "Criminal motivation on the dark web: A categorization model for law enforcement". In: Digital Investigation 24 (2018), pp. 62–71.

[2] Mauro Conti et al. "A survey on security and privacy issues of bitcoin". In: IEEE Communications Surveys & Tutorials 20.4 (2018), pp. 3416–3452.

[3] Gengqian Zhou et al. "A market in dream: the rapid development of anonymous cybercrime". In: Mobile Networks and Applications 25.1 (2020), pp. 259–270.

[4] The State of Ransomware. 2021. url: https://secure2.sophos.com/.

[5] Crypto-Ransomware Attacks: The New Form of Kidnapping. 2015. url: https://blog.trendmicro.com/crypto-ransomware- attacks- the new-form-of-kidnapping/.

[6] Annual number of ransomware attacks worldwide from 2016 to 2020, 2021. URL: https://www.statista.com/statistics/494947/ransomwareattacks-per-year-worldwide/.

Money laundering is indeed the practice of disguising the source of illegal funds (such as the proceeds of crime), typically through a complex commercial transaction.

Trafficking in illicit firearms and other weapons: It is well documented that the dark web has been abused to enable such trades, with cryptocurrency serving as the means of exchange.[7] For instance, the dark web firms have boosted the overall accessibility of firearms for the same price as the illegal market on the street, according to a 2017 RAND Europe study on the international trade in firearms.[8] It is well documented that bitcoins are often used to purchase commercialized child pornography, assault, and exploit materials and/or services (such as over a webcam).[9]

Contract Killers: There are numerous underground websites where one can hire a hitman to kill someone else. For instance, a White-hat hacker by the name of "bRpsd" is said to have assisted the FBI in May 2016 in the capture of numerous hitmen by breaking into the "Besa Mafia" website on the dark web and exposing contract data including user accounts, client communications, and other details. The cost of a murder service reportedly varied between $5,000 and $200,000 on this secret website that connected clients and hitmen. Additionally, it was stated that one may pay a contractor 500 dollars to kidnap (instead of killing the victim) or $1,000 to put a targeted car on fire.[10]

Human smuggling: This is an online black market where criminals use secret websites to sell services related to human trafficking, such as organ or slave trafficking. According to the U.S. State Department,[11] there were 118,932 victims of human trafficking in 2019. However, only 11,841 traffickers were prosecuted with only 9,568 successful convictions. It has been also observed that most of the traffickers utilize tools such as encryption and constantly switch between profiles and sites on the dark net to avoid being tracked by law enforcement agencies.

[7] Abeer ElBahrawy et al. "Collective dynamics of dark web marketplaces". In: Scientific reports 10.1 (2020), pp. 1–8.
[8] International Fire arms trade on the dark web. 2021. url: https://www. rand . org / randeurope / research / projects / international - arms - trade-on-the-hidden-web.html.
[9] Bruno Requi˜ao da Cunha et al. "Assessing police topological efficiency in a major sting operation on the dark web". In: Scientific reports 10.1 (2020), pp. 1–10.
[10] How a bitcoin white hat hacker helped the FBI catch a murderer. 202. https://bitcoinmagazine.com/
[11] Beating Human Trafficking on the Dark Web. 2021. https://cobwebs.com/en/press-releases/human-trafficking-on-dark-web/

Drug trafficking: Similar to other illegal activities, drug traffickers (suppliers) & addicts (consumers) can buy and sell narcotics anonymously on the dark web using cryptocurrencies like Diamond, Bitcoin, Ether, and Ripple. In a joint operation combining the United States (DEA, FBI, and IRS), German, Denmark, Moldovan, Australia, and Ukraine, "Dark Market. Onion" was the biggest online drugs black market that had been shut down by police agencies, according to Europol's January 2021 report. The number of users, dealers, and transactions on the "Dark Market" was also disclosed to be +500,000,000. More than 4,650 Bitcoins and 12,800 Monaro tokens were exchanged in these transactions. Hacker community services: There are numerous online hacking forums or communities that offer underground markets for selling various tools or services, as well as stolen or leaked information.

HOW TO USE THE DARK WEB

No idea is more notoriously associated with the internet than the dark web. The dark web is undoubtedly considerably bigger than the open and deep web, despite the fact that its scale cannot be determined. Figure 1 shows how Tor, sometimes referred to as an onion router, is utilised to explore the dark web in depth.[12] It is unquestionably the most practical and maybe the safest option, despite the fact that it is not the only one. In addition to the Tor browser, there are several additional ones that may be used to access the dark web, including Freenet, Whonix, Subgraph OS, and I2P (Invisible Internet Project). But Tor is the subject of this essay.

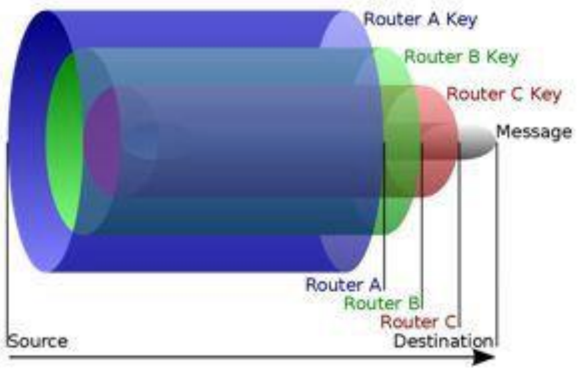

Figure1: the onion router

Obtaining the Tor browser, which works like any other browser, is now the simplest way to use Tor. Tor assists us in rerouting even our user requests through several proxy nodes distributed across the globe that are selected at random. In this manner, your connection won't be linked to you.[12]

Features of a Tor Browser:

1. It includes the Tor project and the Firefox browser.
2. The Tor browser is free software.
3. Client-side automatic data decryption.
4. The internet traffic is directed using an overlay network.

The benefits of using the Tor Browser:

1. Hides users' IP addresses to protect their privacy.
2. This browser opens web pages that are encrypted and secured.
3. One advantage of utilizing Tor is anti-spy protection, which stops third parties from monitoring the sites we visit.

Consequences of Utilizing Tor Browser:

1. Network connectivity is a significant issue with the Tor browser.
2. Large files cannot be downloaded or uploaded with this browser.
3. The security of this browser is a concern because the exit node contains information about the sites that are viewed.

TOR IN A NUTSHELL

The most well-known program used is called The Onion Router (Tor). For anonymous and covert networking. A network of servers that are willing to serve as volunteers transfer data for Tor's operation. The Onion Router gets its name from the fact that it encrypts data with multiple layers of encryption before transmitting it via the network, removing each layer one by one as it travels along the randomly selected path.[13] Its number may exceed 3000 servers.[14] In the 1990s, the U.S. Navy created Tor intending to safeguard online

[12] Inside the Dark Web – Erdal Ozkaya, 2019

[13] S. V. M. v. S. Martijn Spitters. (2014). Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services, Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint, p. 220-223, 24 September 2014.

[14] Gareth Owen. N. S. (2015). The Tor Dark Net, 30 September 2015. https://www.cigionline.org/publications/tor-dark-net.

communications for American intelligence. They were formally introduced to the public in 2002 with the primary goal of enabling open-source data gathering.[15]

Despite the primary objective of creating such a network, the Tor network evolved into the ideal location for many sites to plan criminal and dangerous operations while maintaining the anonymity of their users. Along with Black Market Reloaded (which has been shut down by its administrator in December 2013), Agora, and Pandora, Silk Road was one of the most well-known online marketplaces. It was shut down by the FBI in October 2013 but reopened after just one month. Some of these websites are simple to locate simply browsing certain network pages.

These pages function as dictionaries with lists of links to these sites, similar to Hidden Wiki, or by using specialized but sporadic search engines on the Tor network, similar to DuckDuckGo, Tor Search, and Grams. However, all of these resources only cover a very small subset of the private networks on the network. Tor operates differently on the TCP transport layer and employs a socket connection-based communication method. When a new user, known as a "source," enters the network using the Tor browser, Tor creates a virtual loop with several network nodes that are selected at random. It uses this virtual network for around 10 minutes before constructing another one and continuing in this manner.[16]

There are three different sorts of nodes in the circuit:

1. Nodes in the network and the one that receives incoming traffic are known as the entry node.

2. Pass the information from one device to the following using intermediate nodes.

3. Exit Node: This node, which completes the circuit, sends communications to the public internet.

When a "source" requests access to a site, Tor encrypts the request with multiple layers of encryption, delivers it to the relevant, then routes it over several randomly selected intermediate nodes that are dispersed throughout the world. The encrypted request is

[15] R. F. B. M. J. M. G. D., Ahmed, Zulkarnine, T. (2016). Surfacing Collaborated Networks in Dark Web to Find Illicit and Criminal Content, Intelligence and Security Informatics (ISI), 2016 IEEE Conference, p. 109-114, 28 (September).

[16] Ahmad, I. (2018). A New Look at the TOR Anonymous Communication System, Journal of Digital Information Management, 16 (5) 223-229, (October).

decrypted by one layer with each jump to a node before being forwarded to the subsequent intermediate node. When the exit node receives the request. With this approach, all source information is lost, the user's identity is unclear, and only the final nodes in the circuit can be reached in the event of a return.[17] Additionally, Tor enables the deployment of websites that use the "onion" suffix and cannot be processed or rendered outside the Tor network without disclosing the location of the hosting servers. Together, these features enable anonymous browsing and turn it into a secure method of user interaction.

HOW TO TAKE PRECAUTIONS FROM THE DARK WEB

Your device connects to the internet over a secure tunnel called a VPN, as well as a virtual private network. It gives people freedom online while protecting against censorship, interference, and online snooping. Your internet traffic travels through an encrypted channel when you use a VPN, rendering it undetectable to hackers, authorities, or even your internet service provider. It creates a safe link to a VPN service, which serves as an intermediary for your online activity. By doing this, you can prevent websites, applications, and other services from tracking your online activities or discovering your real IP address.

VPNs offer a wide range of advantages:

1. Alter your location: By changing your IP address with a VPN, you might appear to be online from a different nation. You can use this to access services and content that are restricted by area.

2. Protect your private information: A VPN hides your identity from websites, applications, and other organizations that try to monitor your online actions. Strong encryption also prohibits your internet service provider as well as other potential listeners from seeing their browsing patterns.

3. Boost security: VPNs protect your connections from security risks including packet sniffing, unauthorized Wi-Fi networks, or man-in-the-middle attacks. A VPN guarantees that your data is secure whether you're a traveler, a remote employee, or someone who uses public Wi-Fi.

[17] ibid

Every time your privacy is crucial to you, a VPN should be used. Without interrupting your online activity, the software runs in the background on your device. Here are some additional instances where a VPN is particularly helpful:

- When traveling: Regardless of where you are physically located, a VPN enables users to browse the web anonymously and securely.
- When you're having fun: Use the internet without being concerned about restrictions placed on your internet provider or neighborhood Wi-Fi network.
- When using public Wi-Fi: Using public Wi-Fi hotspots in places like cafés, airports, and parks can put your data in danger. In these circumstances, a VPN offers high encryption protection for your data.
- Gaming: To lower ping, protect oneself from DDoS attacks, & play with friends from other countries, link to VPN servers that are close to gaming servers.
- File-sharing: Download files without revealing your identity and shield your IP address from prying eyes that might monitor your downloads.
- Online stores that display varying prices depending on your location can be accessed using a VPN to find the greatest offers around the world.

Let's investigate how a VPN functions now:

Your internet connection behaves differently if you don't use a VPN. Your internet provider (ISP) uses your particular IP address to connect you to a website when you access one. As a result, your ISP will be able to track your online behavior and connect it to your Port number. On the other hand, when you use a VPN to access the internet, the VPN app in your device creates a secure connection with a VPN server. Your ISP still receives your traffic, but it is no longer legible to them. Only the IP address of the VPN server, which is shared by many users and frequently changes, is visible to the websites you visit. Here are some key concepts related to VPN that will help you understand how it works:

1. Proxying: A VPN server represents your online activity as a stand-in. Websites view the IP address & location of a VPN server rather than your actual IP address & location, which increases your anonymity.

2. Authentication: By confirming their identities & prohibiting illegal access, authentication makes sure that the VPN client and the server can connect securely to one another.

3. Tunneling: VPNs use encryption and tunneling to secure the connectivity between your browser and the network. Each data packet is encapsulated within another packet through the use of tunneling, which makes it more difficult for outside parties to intercept.

4. Data is encrypted in the VPN channel because only the intended receiver may decrypt it. This guarantees the anonymity and privacy of your web traffic, even from your ISP.

Different protocols are used by VPNs to connect to VPN servers. As an illustration, Express VPN provides Light Way, a method that excels in terms of speed, dependability, and security. OpenVPN, IKEv2, L2TP/IPsec, & Wire Guard are some further well-liked protocols.

SOME DARK WEB CRIMES THAT SUCCESSFULLY TAKEDOWNS

After the 2015 Paris attacks, the amorphous hacker collective Anonymous began an Operation Paris (OpParis) campaign, which resulted in the removal of hundreds of ISIS-related websites from the dark web.[18] According to a United States Department of Justice (DoJ) update on May 24, 2021, Kirill Victorovich Firsov, a citizen of Russia, was sentenced to 30 months in prison for his role in trying to sell stolen card information & other data on the dark web, which was then used to carry out other criminal activities.[19] Firsov oversaw a website that offered services and personal data that had been stolen.

Slilpp, a Tor-based Dark Web marketplace, was shut down on June 11, 2021. Slilpp, which gave its customers access to up to 1,400 sites, 80 million accounts, and services globally, was in charge of trading stolen credentials over the darknet. An individual from Ukraine who was a part of the cybercrime organization FIN7 was transferred to the US in June 2019 and after being detained in Spain the previous June received a seven-year jail term and a $2.5 million fine.[20] And over $1 billion in assets belonging to US persons and organizations were stolen by the group and sold on the dark web.

On June 28, 2021, Ukrainian police said that Binance's cutting-edge data analytics had assisted in finding a group of such money launderers known as FANCYCAT who had been

[18] Abby Ohlheiser, "What you need to know about Anonymous 'war' on the Islamic State", *The Washington Post*, November 17, 2015.
[19] Russian Hacker Sentenced to 30 Months for Running a Website Selling Stolen, Counterfeit and Hacked Accounts, Department of Justice, U.S. Attorney's Office, Southern District of California, May 24, 2021
[20] High-Level Member of Hacking Group Sentenced to Prison for Scheme that Compromised Tens of Millions of Debit and Credit Cards, Department of Justice, Office of Public Affairs, June 24, 2021.

involved in several criminal schemes, including the "Clop ransomware" scam and the laundering of funds for dark web operators.[21]

The Moroccan police, acting as part of Operation Lyrebird, detained a suspect on July 6, 2021, who was suspected of being involved in several cyber-frauds against banks, telecom companies, and multinational enterprises.[22]The suspect launched malware attacks against the company network of French-speaking communications businesses, targeting thousands of innocent people using phishing, credit card fraud, and other means. On July 13, 2021, all access to Revil gang-related dark web data sites was lost. It was assumed that either the gang broke apart on its own or restrictions enforced by law enforcement organizations were to blame. The enormous global ransomware attack on the Kaseya IT software solutions that occurred on July 2 is attributed to the Revil gang of cybercriminals.[23]

WHAT ARE RED ROOM AND SILK ROAD IN THE DARK WEB?

Red Room: According to urban legends and myths, red rooms are unreal. According to the legend, users can watch rapes & murders live on "Red Room" sites on the dark web for hundreds of dollars. On the "dark web," there is a secret website or service where users can watch interactive torture or death take place or take part in it. A secret network of websites only accessible using a specialized web browser is known as the "black web." It's being used to maintain the privacy and anonymity of online activities, which is useful for both legitimate and illicit uses. It is known that some people use it for very criminal acts, even though some utilize it to avoid government censorship. You need to use the Tor anonymous browser to access the dark web.[24]

The Silk Road had been a system of historic trading routes. The Silk Road's extensive trading networks transported more than simply goods and riches. A tremendous transfer of knowledge, ideas, culture, and beliefs was brought about by the constant migration and population mixing, and this had a significant impact on the history & civilization of the

[21] John Leyden, "Binance reveals how data analytics led to ransomware-linked money laundering bust', PortSwigger, June 28, 2021.
[22] Moroccan police arrest suspected cybercriminal after INTERPOL probe, Interpol, July 6, 2021.
[23] Cameron Camp and Aryeh Goretsky, "Kaseya supply-chain attack: What we know so far", *WeLiveSecurity*, July 3, 2021; Latest ransomware attack appears to hit hundreds of American businesses, *The Guardian*, July 3, 2021.
[24] Inside the Dark Web – Erdal Ozkaya, 2019

Eurasian persons.[25] Due to the substantial silk trade that existed at the time, it was given the name Silk Route. Until the creation's secret was revealed, China held a monopoly on the production of this priceless fabric. In addition to facilitating commerce in silk, the route also promoted trade in plenty of other textiles, different varieties of spices, grains, fruits, and vegetables, as well as in animal skins, woodworking, jewelry, precious stones, and other valuables.[26]

STATISTICS OF THE DARK WEB IN INDIA

Comparing Australia & South America to India and the dark web, respectively, India has the largest market of users. 26 percent of the country's total dark web users are from India. According to ZDNet, the ShinyHunter hacking collective attempted to sell 73 million users' data on the dark web. Around ten businesses had their security compromised, including the South Korean fashion portal Social Share, printing provider Chat books, and online dating app Zoosk.

Around 500,000 Zoom accounts were compromised in April 2020 & sold for less than a rupee each, claims cybersecurity company Cyble. According to Arxiv, just 29.4% of female users of the dark web were discovered to be male, whilst 70.6% of visitors were male. According to Arxiv. If we take the category-wise statistics, we can summarize them below from the table.

Category of age	Percentage of the dark web usage
18-25	35.9%
26-35	34.8%
36-45	16.8%

[25] Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. Calif. L. Rev., 107, 1753.

[26] Martin, J., Munksgaard, R., Coomber, R., Demant, J., & Barratt, M. J. (2020). Selling drugs on darkweb cryptomarkets: differentiated pathways, risks and rewards. The British Journal of Criminology, 60(3), 559-578.

46-55	8.8%
Above 55	3.7%

The dark web is not an awful place to browse, but it still poses a risk and is not a secure environment. Some websites are trustworthy, and visitors can gain something from them. However, let's take a closer look at how legal access to the dark web is in India.

The legality of the dark web in India: Yes, it is allowed to surf the dark web in India. Nothing can prevent you from utilizing it. We learned about the darknet and how it works above. After that, we realized that India considers surfing the dark web to be legitimate. It's a common misperception that only illegal activity may be conducted on the dark web. That is partly accurate. The dark web also offers several benefits. The dark web is used by individuals for a variety of activities, including reading books, gathering information, having private conversations they don't want others to see, and even for official investigations into crimes by activists, journalists, as well as other government authorities.

The reason why the Dark web is legal in India: In India, using the dark web was permitted. Because this is just another area of the internet you are browsing through TOR, Freenet, etc., even the Indian government doesn't view it as unlawful activity. This does not, however, imply that you are unrestrained. Certain restrictions should surely be followed when browsing the dark web. If you chose to open the universe of the dark net, keep in mind that one incorrect click could endanger your life. On the dark web, the majority of shady crimes take place, and there is a clear distinction between what is lawful and illegal when using the dark web.

LAW MADE BY THE INDIAN GOVERNMENT TO REGULATE SUCH CRIME THROUGH DARK WEB

Additionally, Article 21 of the Indian Constitution grants citizens the right to access the Internet. In essence, the court stated that these right forms the foundation of freedom of expression & religion. As a result, we are unable to prevent someone from using the website because doing so would violate their right to free speech. We are aware that it is allowed to use the dark web in India, therefore this presents unique difficulties for law enforcement. In addition, there are no strict rules governing cyberspace in India. The laws in our country have many flaws, and the dark web has its special issues. Indian Information Technology Act, 2000 only contains six sections that deal with cybercrimes in India. People tend to click on the links they find while browsing the internet. But you shouldn't utilize the dark web recklessly. You may end up in jail with just one click. Five Mumbai students were busted while dealing in the acquisition of drugs via the dark web, according to a report in the Indian Express. The 1,400 LSD dots that these five students purchased cost 70 lakhs.

They have placed the order with such a cartel from the Western European nation on behalf of a US friend who was part of a dark web syndicate. He provided the Mumbai address to which the LSD dots have been sent. As per Bombay DCP (Anti-Drugs Cell) Shivdeep Lande, conducting an arrest is a challenging process because of the sophisticated design of the dark web version, thus these 5 students were detained after the packages were delivered. Additionally, a lot of anonymity-related capabilities are provided, making it challenging to find the culprits. Employees of the US Naval Research Laboratory created the dark web in the middle of the 1990s to shield US intelligence communications. Although it was created with good intentions, it eventually turned into a location for criminals to carry out their ill-intentioned acts.

CONCLUSION

TOR and other Dark Web networks have given bad actors various opportunities to trade "goods"—both legal and illegal—anonymously. In terms of criminal services and activities, the dark web is a rising asset. Security systems should be on the lookout for these issues and take action to fix them. Law enforcement & policymakers now face a hurdle in effectively combating bad actors that are active in cyberspace due to the increasing technologies with encryption (privacy) and anonymity (such as the Dark Web as well as its specialized software). A dark website is a system of thousands of sites that mask their IP address using anonymizing software like Tor and I2P. The dark web, which is most well-known for being used for child pornography and even the selling of illegal drugs, also allows for anonymous whistleblowing and shields users from government monitoring and control. Action must be taken to handle the problem of the dark web's encryption to safeguard people's security and privacy. The majority of unlawful and destructive acts are carried out on the dark web thanks to the anonymity offered by sophisticated algorithms that secure users' identities and erase any evidence of their presence on websites. The sheer complexity of regulating the dark web led to the creation of markets for drugs and weapons as well as vast networks on websites used for propaganda and communication by terrorists. Between anonymity for the sake of security & anonymity as a covering for illicit activity, there is a delicate line. The encrypted aspect of the dark web presents a significant barrier for the governments, thus developing new strategies for monitoring and thwarting nefarious activity on the dark web has to be a top priority for all nations.