International Journal of Advance and Innovative Research
Volume 8, Issue 1 (II) January - March 2021

ISSN 2394 - 7780

AN ETHNOGRAPHIC STUDY OF DARKNET

Bhakti Chaudhari and Sumathi Rajkumar
Department of Information Technology, Nirmala Memorial Foundation College of Commerce and Science, Mumbai, India

ABSTRACT

With the advent of the technical era, the tunnel of the World Wide Web became denser and more sinister. Some portion of the WWW is full of derelict URLS, stolen credentials, malware, phishing kits, forbidden drugs, weapons, and other illicit goods that are traded among anonymous buyers and sellers. It is notoriously known as "Darknet". Open exchange and the use of virtual cryptocurrencies made the darknet more popular among criminogenic users. Darknet requires the use of special browsers providing access to anonymous networks and the most popular browser among all to enter the darknet is TOR. An ethnographic study of this paper highlights the recent incursions of Darknet along with its existing dark shadows on society. It also accentuates the bright side of the Darknet that attempts to provide a think tank to academicians, researchers and many individuals of the society before they use any browser or services that supports anonymity and privacy. It will definitely help us to minimize the adverse impact of the darknet on society.

Keywords—Darknet, Anonymity, Cryptocurrencies, TOR, privacy

I. INTRODUCTION

Back in the 1960s, when ARPANET was flourishing with its glory of communications over the internet, two organizations in the US Department of Defence tried to develop a secrete encrypted network that would protect the sensitive Communications of the US Spies. The ultimate aim to design such a communication network was to enable human activists and people to communicate and collaborate, remotely and securely. But soon in the 1970s ARPANET discovered an illegal use of this network when the students of Massachusetts Institute of Technology and Stanford University traded drugs using its Artificial Intelligence Laboratory. With a fear of losing privacy, ARPANET was divided into MILNET(Especially used for Military Operation and communications) and Civilian network(used by the general public). This civilian network took the form of the internet. After the release of the Internet in the 1980s, the world became more and more connected. In 2000, Ian Clark, a computer scientist implemented his project into a free software called 'Freenet' and made it available to the public. In a short period, several copies were downloaded. After a continual development of the software several versions were released, and slowly it became fundamental support for 'Darknet'[1]. When an internet user switches to pure darknet operations, Freenet becomes very difficult to detect from the outside world. The transport layer of this network uses a special routing mechanism termed as 'Onion Routing' [2,3]. It's a process in which a message is encrypted after every transfer through a node or a router. These layers of encryption are similar to the peels of an onion. Due to these multiple encryptions, the identity of the sender and receiver remains unknown. In 2002, Tor- The Onion Router, a private Internet browser, was finally released to the world. With Tor, people can freely browse online maintaining anonymity. The hidden imprints and anonymity led many Nation-State Actors, State-Sponsored Hackers, pornographers, scam artists, drug, and gun dealers to find their home for some clandestine activities. And slowly the Darknet became the hub of international criminal activities [4,5].

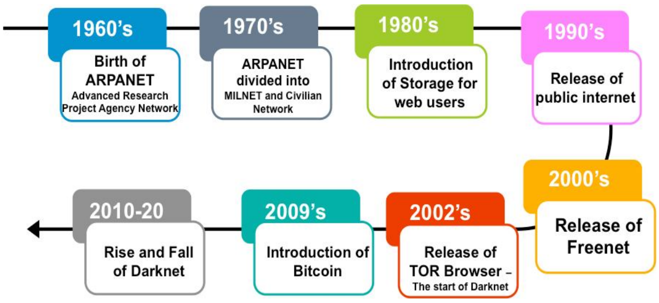


Fig 1: Timeline of Darkweb

II. LAYERS OF INTERNET

The Internet is an ocean of information. Every individual read topics according to their interest and gain information. It's a mesh of variety of networks (some are guided by VPN whereas some are open) and many other devices connected to share information all over the world. It is divided into three categories: Surface web, Deep web, and Dark web.

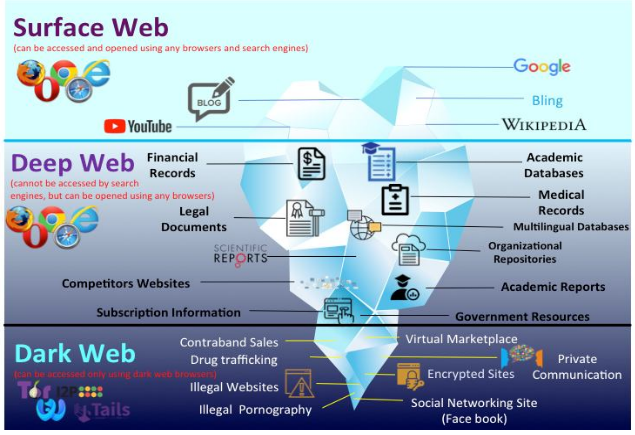


Fig 2: Layers of Internet

A. *Surface Web*

The surface web is that stack of information, which is readily available to all people and searchable with any standard search engines such as Google or Bing or Yahoo. Normally pages defined under surface web are said to be 'indexed'. It is also knowns as **'Clearnet' or 'Visible net'**. The interesting thing is that the surface web is merely 10% of the whole web [6,7].

B. *Deep Web*

Some pages of the web require credentials to access like emails, cloud service accounts, banking sites, subscription-based online services, companies' internal networks and their databases, education and certain government-related pages, etc. Such pages are neither indexed nor visible on access by any search engine. They do not use common domains like .com, .gov, and .edu,. The layer of the internet that consists of such pages is termed as '**Deep Web**'[6,8,9]. The estimated size of the deep web is beyond 90%.

C. *Dark Web*

The third layer of information and pages that are not indexed but hosted anonymously. Such information is accessible through "overlay networks", which run on top of the normal internet and provide hidden access. Special software or browsers are necessary to access the dark web because a lot of its information is encrypted. The most popular browsers are TOR(The Onion Router) and I2P[10].

Considering the infographic of Ocean surface and Iceberg as shown in fig: 2, the Surface web can be imagined as the area of an iceberg that is above the ocean surface whereas the portion of the iceberg below the ocean surface is the deep web, Dark web would be the deepest point of the submerged iceberg. The deep web and dark web are functionally different, but these two terms are mostly used interchangeably.

III. SUPPRT OF TOR AND I2P

The dark web is a concealed subset of the deep web that is requiring a specific browser to access. It is used to describe a collection of websites, which are visible only through the Tor or I2P browser[11,12,13].

TOR browser routes all web traffic through the TOR network. It consists of 'n' layers of encryption that pass through multiple relay points in between. From an entry point till the final destination i.e. an exit node, data traffic bounces through randomly selected middle relay. TOR websites and browsers identify user's connection but efficiently protects his/her identity. This feature of anonymity increases the number of users on the darknet. TOR supports the search of '.onion' websites that are available only in anonymous TOR browser.

I2P (Invisible Internet Project) is another anonymous communication system available. It uses I2P router on user's device, which enables temporary, encrypted, one-way connections with other I2P routers. Web traffic passed along with these connections are protected by a cryptographic method called as 'garlic encryption'. Anonymous websites of I2P are called "Eepsites". These sites have an extension '.i2p' and are hosted using built-in tunneling application. I2P serivces also supports SAM (Simple Anonymous Messsaging-a chat application), Susimail (a web based email client) and I2P Snark (a Bitorrent Client).

Because of the obscure nature of the web and anonynous supports of browsers, the Dark web is mainly known for its activities linked to criminal intent or illegal content [2]. The dark web has many gray shades of activities. It is badly known for its hidden marketplaces, sale of illicit items ranging from drugs, weapons to extinct animals, malware, human trafficking, and pornography. The anonymity of the dark web is more inclined towards criminogenesis. Many Government Law Enforcement and private cybercrime agencies are working hard to shut down such websites. But it also has its bright side. The dark web is also famous for its secure email services, blogs, clubs and many forums. Many Reporters recommend the use of 'TOR' for bloggers, journalists, and activists in countries where open discussions on certain topics are banned. Facebook and BBC news channel have also recently launched its 'TOR' version. There are also some SINs- Strategic Intelligence Networks that help people to manage through a crisis. In this paper, we would like to flash a light on such activities and highlighting a few recent attacks of Darkweb.

IV. DARK SHADOWS WITH SOME RECENT INCURSIONS OF DARKNET

Darknet's activities are more inclined towards infringement. Some shadowy domains of the darknet and few recent attacks of the darknet are listed here:

A. Virtual Marketplace

Due to anonymity, security, and privacy the dark web showed its potential to host an increasingly large number of malicious services and activities. And soon it became famous among illegal traders. A virtual market, also known as a dark web Marketplace specialized in the trading of illegal and illicit goods that includes drugs that require pharmaceutical prescriptions, stolen credentials, weapons, extinct animals and many more. The report published by Positive Technologies showed that crypto miners, hacking utilities, botnet malware, RATs(Remote Access Trojan), and ransomware Trojans are widely available in the shadow cyber services market, while the highest demand is typically for malware development and distribution [14].

Customers associated with such markets transact with the use of cryptocurrencies. It's a digital or virtual currency designed to work as a medium of exchange. Bitcoins, Monero and litecoins are some of the common cryptocurrencies.

Bitcoin is the most commonly used digital decentralized cryptocurrency that uses anonymous, peer-to-peer transactions. Traders across the marketplaces are using bitcoins as a medium of payment. Bitcoins are further exchanged in traditional currency, or "mining" them. Every financial transaction of a bitcoin is recorded in a public ledger, called the blockchain. The information recorded in the blockchain is the bitcoin addresses of the sender and recipient. An address does not uniquely identify any particular bitcoin; rather, the address merely identifies a particular transaction.[15]

With the incredible efforts of many governments and law enforcement, several virtual market places are shut down. One of the most wanted marketplaces "Silk Road" was taken down by the US Federal Bureau of Investigation. However, after few months SilkRoad2.0 quickly regained all the fame in the Darknet and that resulted in the conviction of Ross Ulbricht, the owner of SilkRoad. He later sentenced to life in prison without the possibility of parole. But the roots of anonymity are so strong that SilkRoad3.0 is popped up and that where we are today [12,16]. Due to this Silk Road became a case study for many researchers, academicians, and cybercrime investigators to hunt for more marketplaces.

From 2015-2017, Worldwide law enforcement investigations seized a few more leading marketplaces namely, AlphaBay, Bloomsfield, and Hansa. With a fear of getting indicted, some marketplaces were closed down with exit scam. The most recent seizure in May 2019 was of WallStreet Market which had around 10,000 listings.[17]

According to Digital Shadows, There are still few Automated Vending Carts (AVCs) that exist in the dark web that trade credit cards, credentials and access their trades. These AVCs remained unaffected by all other international seizures.[18]

B. Child Pornography

The majority of traffic to hidden Dark Web sites using TOR is for viewing and distributing images of child abuse and purchasing illegal drugs. According to the research of Dr. Gareth Owen and Nick Savage, at the University of Portsmouth, a huge amount of TOR traffic was related to child abuse and pornography [12,14]. Many law enforcement authorities have taken efforts to eradicate child pornography websites. They had taken covert measures to shut down the leadership of these websites, also arrested the organizers and core members. Despite many efforts by private cybercrime agencies, these websites are still popping up. It's been observed that child pornography websites have been operated and maintained with high secrecy based on the anonymity that the darknet provides.

In February 2015, the FBI took down the infamous Dark Web site 'Playpen', which hosted more than 23,000 child pornographic images and videos and had more than 215,000 users [12,19].

In November 2016, U.S. Immigration and Customs Enforcement's Homeland Security Investigations and the High Technology Investigative Unit of the Child Exploitation and Obscenity Section (CEOs) seized "Giftbox Exchange" along with a subforum "Babies & Toddlers". This site was organized into different forums for posting different types of child pornography which were categorized by age of the minor victims, It had more than 72,000 registered users and 56,000 posts. In addition to operating the site on the TOR network, the owner Mr. Falte and his co-conspirators used other advanced technologies for encryptions to ruin law enforcement efforts.[12,19]

The most recent seizure of the child pornographic website is the shutdown of 'Welcome to Video' [20]. This site is said to the world's "largest dark web child porn marketplace". Users of this website could purchase videos using cryptocurrency and an annual membership was priced at 0.03 bitcoins. The international investigations led by the IRS-CI (Internal Revenue Service, Criminal Investigation (IRS-CI) is the United States' federal law enforcement agency), U.S. Immigration and Customs Enforcement (ICE)'s Homeland Security Investigations (HSI) and the NCA. A federal jury in the District of Columbia accused a South Korean national named Jong Woo Son. The Korean National Police of the Republic of Korea, the National Crime Agency of the United Kingdom assisted and coordinated with their parallel investigations.

C. Coronavirus Pandemic and Dark Web

With an intensified sense of fear caused due by the global pandemic, marketplaces on the dark web have seen a rise in Covid-19 related products such as N95 masks, gowns, gloves, the drug chloroquine, and other services. Sought-after have all been listed on these marketplaces. Security software firm IntSights found blood allegedly belonging to recovered coronavirus patients was even being offered for sale.[21,22]

Besides, many services and products, phishing kits are also being offered at discounts in "coronavirus sales". A threat intelligence analyst Liv Rowley at Blueliv, a computer, and network security firm stated in her BBC report that – Such discounts are offered because many cybercriminals believe that Pandemic is the right time to earn money and spread these phishing kits.

D. Zoombombing

In 2020, the outbreak of the coronavirus led to the worldwide pandemic, and the entire world got halted. It forced many people from various organizations, enterprises, schools, and universities to stay at home and work remotely. Since then video conferencing became an ultimate solution to connect with remote people, workers, customers, employees, and students. 'Zoom' was the more popular video conferencing software among all. In April 2020, many users of Zoom experienced a persistent "Zoom-bombing"[23,24], a new kind of attack within which unsolicited participants enter video meetings and shout slurs and threats in an endeavor to disrupt their meeting. Zoom bombing had left online lectures vulnerable to many universities. These attacks have brought attention not only to the dearth of security on video conferencing platforms, but also the ignorance towards the software vulnerabilities [23,24,25]. US-based Cyber-intelligence firm 'Cyble' reported that several free Zoom credentials, approximately half-million being offered on hacker forums on the Dark web around April 2020 as some way for hackers to extend their notoriety. However, this company was able to obtain about 530,000 accounts for about US$0.002 each, Credentials were ranging from email and password to meeting IDs, names, and host keys [26,27]. Full credentials could be used in a range of activities from Zoom-Bombing to Business Email Compromise (BEC) attacks. During these incidences, it has been observed that these attackers usually created bots to hammer sites with automated login attempts, leveraging credentials from past data breaches. Once the bot hits the correct combination, its operators gain access to the account. Unfortunately, search for such vulnerabilities and the source on the dark web remained obscured.

E. Data Leakage

In May 2020, the leak of nearly 2.9 crore job-seekers' details were discovered by 'Cyble'. Its founder Beenu Arora informed about the leakage of Aadhaar card data on the dark web. A firm has been trying to trace the source of the leak and identify the perpetrators. Meanwhile, Cyble researchers have received anonymous advice that the jobseekers' data leak was the results of an unprotected Elasticsearch instance - a tool that collects data from a large range of locations on the internet with the necessities of the person searching, and allowing the user to analyze large chunk of knowledge in real-time from everywhere the web [28,29].

In November 2020, During the routine observation of the darkweb, Cyble also discovered a data leakage of around 20 million customers of BigBasket, an online grocery shop in India. Details of this leakage included full names, email IDs, passwords, contact numbers (mobile and phone), full addresses, date of birth, location, and IP addresses of where users have logged in from have been put up for sale on the dark web for $40,000. [30,31]

V. FLIPSIDE OF DARKNET

Darknet is not completely illegal although it has its ominous overtones. It has great potential in a variety of domains. There are plenty of services available on the darknet that doesn't break any law of cybersecurity.

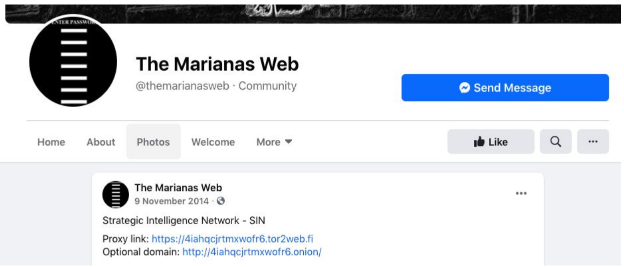
A. Book and Chess Club:

There are many reading communities on the dark web for years. Other than general books, more controversial or forbidden books are made available in the form of book clubs. Even Ross Ulbricht, the founder of SilkRoad had his famous book Club where people discussed literary classics like Ralph Ellison's 'Invisible Man' alongside more controversial books like 'Anarchist Cookbook'. However, Ulbricht's online book club is no longer operational, but there are many more exists on the dark web, Such as 'Jotunbane's Reading Club' and the 'Imperial Library of Trantor'. These sites not only allow users to download illegal copies of popular books but also allow them to have active discussions on certain reading materials. The most popular books available on the dark web are Hacker, Hoaxer, Whistleblower, Spy, Gabriella Coleman's history of Anonymous; Cypherpunks by WikiLeaks founder Julian Assange; and Anarchism and Other Essays by Emma Goldman. All book clubs keep reading the history of all users hidden from other marketers.[15,32]

The dark web also has a chess club named "The Chess". It includes unlimited games against players from around the world and some pen forum to talk about the strategies of this game. There is no cryptocurrency fee and it is fully anonymous.

B. Strategic Intelligence Network

Considering another flip side of the dark web there exists few SIN, Strategic Intelligence Network. It is packed with information on how to deal with any sort of crisis anywhere on earth, from natural disasters to riots or any kind of war. It provides information about the resources and tools to be used in such scenarios. The pathways to lead such SIN is through the surface web. One of the SIN that has its reference on Facebook listed below:



Strategic Intelligence Network - SIN

Proxy link: https://4iahqcjrtmxwofr6.tor2web.fi
Optional domain: http://4iahqcjrtmxwofr6.onion/

Fig 3: Presence of Mariana's Web (SIN) on surface web

C. Social Media and News

Many countries around the globe namely China, Iran, North Korea, Saudi Arabia, Vietnam are known to be the most censored counties. China has the most censored Internet censorship system; it blocks YouTube, Facebook, Twitter, Wikipedia, and many other media channels. Instead, it has its search engine, video hosting platform, and social media sites. Iran has its own tightly secured intranets for schools and universities. Many western platforms and services are forbidden to citizens. Citizens who deliberately access these sites and services over the regular internet will first receive a warning and further may lead to prosecution. As a result of these restrictions, citizens from such countries found their way on the dark web. Anonymity is the only thing such citizens want to have.

In 2014, Facebook, a giant social media platform launched a TOR hidden service. This version is pretty secure; it not only protects the user's local traffic and but also its location. It's also designed to circumvent censorship and surveillance to protect the user's identity from repressive regimes like Iran or China [33,34].

In 2019, BBC(British Broadcast Channel) launched a 'Dark web' copy of its news channel. The sole intention behind this launch was to thwart censorship attempts of many countries. As it is accessible with TOR, it helps users to obscure their identity and what data is being accessed. It helps many users to avoid government surveillance [35].

D. Secure email services

There are several heavily encrypted email services available on the darknet. ProtonMail is among the best known. This end-to-end encrypted service was developed by MIT and CERN scientists and has a presence on the surface web. Like many other aspects of the darknet, these email services provide the most secure and anonymous way of communication. For example, one might set up ProtonMail to create a darknet chess account or an account for some blogs.

E. Other Beneficiaries

There also exist some forums for journalists, national activists, political protestors, bloggers, and whistleblowers to express their views. For these individuals, the Dark Web provides a way to elude censors and keep them safe from the prying eyes of the state.

Back in 2013, The Guardian revealed that the National Security Agency (NSA) had been monitoring the phone calls of American citizens both within the US and between the US and other countries, whether or not they were suspected of a crime [31]. Journalist Edward Snowden leaked many of the revelations that helped to unmask NSA surveillance. The Dark Web has proved so useful to whistleblowers that the CIA – Central Intelligence Agency itself launched a Tor-based site to receive leaks from its sources. [36]

The dark web is a deep valley of knowledge for some academic researchers. Resources of the dark web such as Sci-Hub offer free access to millions of academic research papers. The American Journal of Freestanding Research Psychology (AJFRP) became the first free and open Darknet academic journal.

VI. AWARENESS STATISTICS OF DARKWEB IN WOLRD WIDE

TOR/I2P hides the IP address and location of the user. As a result, it is impossible to get an exact usage count of the dark web users from each country. ‘Statistia.com’ presents a statistic of internet users who have accessed darkweb technologies as of February 2019, sorted by country. During the survey period, 26% of respondents from India stated that they had used such technologies.[37] Although the highest count among all countries is undeniable, but every aspect has two sides as stated above in the paper. Some individuals are using it just to maintin their privacy where as others are using it to fullfill their criminogenic activities.

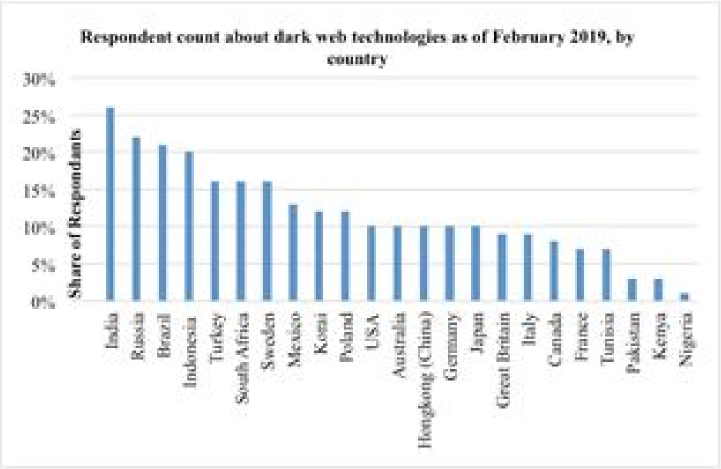


Fig 3: Awareness statistics of darkweb across the world

VII. CONCLUSION

The reality of the Darknet or Darkweb is much more complicated. Due to the lack of academic support, dark web resources are usually inter-cited and it has always been portrayed as a place of mysterious activities, Although, there exist some services that don't run afoul of the law. This paper states both positive as well as negative impacts of the darknet on society. Government’s Law enforcement and private cybercrime agencies have always been trying to track down felonious sites but anonymity rocks every time. Through this paper, we would like to covey that, Darkweb is a double- edged sword. It is as evil or good as we make use of it. Helping journalists and whistleblowers, fighting against repressive regimes, protecting the privacy of an individual are the most important features of the darknet. Whereas, anonymous communication gives the home for hackers, attackers, pornographers and illegal traders. It is highly required to provide more awareness about the darknet to minimize its murky impact on society.

VIII. REFERENCES

[1] Clarke Ian, Sandberg O., Wiley B., Hong T.W. (2001) “*Freenet: A Distributed Anonymous Information Storage and Retrieval System*”, Federrath H. (eds) Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science, vol 2009. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44702-4_4

[2] Goldschlag David, Reedy Michael, & Syverson Paul (1999) “*Onion Routing for Anonymous and Private Internet Connections*”, Communications of the ACM, vol. 4, Issue No. 2, pp. 39-41, ISSN No. 0001-0782. https://dl.acm.org/doi/10.1145/293411.293443

[3] Hsiao-Ying Huang & Masooda Bashir. (2016) "*The Onion Router: Understanding a Privacy Enhancing Technology Community*", Proceedings of the Association for Information Science and Technology, vol. 53, Issue No. 1, pp. 1-10, ISSN No. 2373-9231. https://asistdl.onlinelibrary.wiley.com/doi/full/10.1002/pra2.2016.14505301034

[4] Biddle P., England P., Peinado M., Willman B. (2003) "The Darknet and the Future of Content Protection", Feigenbaum J. (eds) Digital Rights Management. DRM 2002, Lecture Notes in Computer Science, vol 2696, pp. 155-176, ISBN No. 978-3-540-44993-5. Springer, Berlin, Heidelberg. https://link.springer.com/chapter/10.1007%2F978-3-540-44993-5_10

[5] Beckett Andy (2009) "*The dark side of Internet*". https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet

[6] Lewandowski. Dirk & Mayr. Philipp. (2007) "*Exploring the academic invisible web*". Library Hi Tech. vol. 24, Issue No. 4, pp. 529-539 ISSN No. 0737-8831. Emerald Group Publishing Limited https://doi.org/10.1108/07378830610715392

[7] "*Cybersecurity Spotlight – The Surface Web, Dark Web, and Deep Web*". CIS – Center for Internet Security. https://www.cisecurity.org/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web/

[8] Jayant Madhavan, David Ko, Łucja Kot, Vignesh Ganapathy, Alex Rasmussen, & Alon Halevy. (2008) "*Google's Deep Web crawl*", VLDB Endow. vol. 1, Issue No. 2, pp. 1241–1252. ISSN No. 2150-8097. https://doi.org/10.14778/1454159.1454163

[9] Bergman Michael K. (2001) "*The Deep Web: Surfacing Hidden Value*", JEP – Journal of Electronic Publishing, Michigan Publishing, University of Michigan Library. vol. 7, Issue No. 1, ISSN No. 1080-2711 https://doi.org/10.3998/3336451.0007.104

[10] Guccione Darren (2020) "*The State of Cybersecurity: What is Dark web? How to access it and what will you find?*" https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html

[11] "*Browse Privately. Explore freely. Defend yourself against tracking and surveillance, Circumvent censorship*". https://www.torproject.org/

[12] Finklea Kristin (2017) "*Dark Web*", Congressional Research Service. Report No. R44101, Version 9. https://crsreports.congress.gov/product/pdf/R/R44101/9

[13] Dredge Stuart (2013) "*What is Tor? A beginner's guide to the privacy tool*". https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser

[14] Gehl Robert (2014) "*Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. New Media & Society*", New Media & Society. vol. 18, Issue No. 7. https://journals.sagepub.com/doi/10.1177/1461444814554900

[15] Mirea. M., Wang. V. & Jung. J. (2019) "*The not so dark side of the darknet: a qualitative study*", Security Journal. vol. 32, pp. 102–118. https://doi.org/10.1057/s41284-018-0150-5

[16] James Martin, (2014) "*Lost on the Silk Road: Online drug distribution and the 'cryptomarket'*", Criminology & Criminal Justice 2014, vol. 14, Issue No. 3, pp. 351–367. https://journals.sagepub.com/doi/10.1177/1748895813505234

[17] Wikipedia contributors (2020) "*Darknet market*", In *Wikipedia, The Free Encyclopedia.* Page Version ID: 98784200 https://en.wikipedia.org/w/index.php?title=Darknet_market&oldid=987842400

[18] Digital Shadows Analyst Team (2019) "*A growing Enigma: New AVC on the Block*". https://www.digitalshadows.com/blog-and-research/a-growing-enigma-new-avc-on-the-block/

[19] Chertoff Michael (2017) "*A public policy perspective of the Dark Web*", Journal of Cyber Policy, vol. 2, Issue No. 1, pp. 26-38, ISSN No. 2373-8871. https://doi.org/10.1080/23738871.2017.1298643

[20] Department of Justice. The United States (2019) "*Takedown of the largest Darknet Child Pornography Website*", Justice News from Department of Justice, Office of Public Affairs. Press Release Number 19-1,104. https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child

[21] Shah Sooraj (2020) "*Dark web scammers exploit Covid-19 fear and doubt*", BBC News. https://www.bbc.com/news/business-52577776

[22] Tech Desk, The Indian Express (2020) "*Covid-19 test kits, PPE, antiviral drugs, and more; dark web's pandemic sale finds no restrictions*", The Indian Express. https://indianexpress.com/article/technology/tech-news-technology/dark-web-coronavirus-sale-test-kit-covid-drugs-6437182/

[23] Kaplan Ezra & Collier Kevin (2020) "*Passwords and email addresses for thousands of Zoom accounts are for sale on the dark web*", NBC News. https://www.nbcnews.com/tech/security/passwords-email-addresses-thousands-zoom-accounts-are-sale-dark-web-n1183796

[24] Lorenz Taylor & Alba Davey (2020) "*'Zoombombing' Becomes a Dangerous Organized Effort*", The New York Times. https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html

[25] Wakefield Jane, Technology Reporter, (2020) "*Zoom boss apologises for Security issues and promises fixes*", BBC News. https://www.bbc.com/news/technology-52133349

[26] Cuthbertson Anthony (2020) "*Half a Million Zoom Accounts for Sale on Dark Web*". https://www.independent.co.uk/life-style/gadgets-and-tech/news/zoom-app-accounts-sale-buy-dark-web-a9463661.html

[27] Kaplan Ezra & Collier Kevin (2020) "*Passwords and email addresses for thousands of Zoom accounts are for sale on the dark web*", NBC News. https://www.nbcnews.com/tech/security/passwords-email-addresses-thousands-zoom-accounts-are-sale-dark-web-n1183796

[28] Tech Desk, The Indian Express (2020) "*Personal data of 2.9 crore Indian job seekers leaked on dark web*", The Indian Express. https://indianexpress.com/article/technology/tech-news-technology/29-million-indian-job-seekers-data-leak-6424383/

[29] Ians (2020) "*2.9 crore Indian job seekers' data leaked on Dark Web*". https://ciso.economictimes.indiatimes.com/news/2-9-crore-indian-job-seekers-data-leaked-on-dark-web-report/75962658

[30] Mukul Pranav (2020) "*How big is the Bigbasket breach?*", The Indian Express https://indianexpress.com/article/explained/explained-how-big-is-the-bigbasket-data-breach-7026688/

[31] Press Trust of India Ltd. (PTI) (2020) "*Bigbasket faces potential data breach; details of 2 crore users put on sale on dark web*", The Hindu. https://www.thehindu.com/business/Industry/bigbasket-faces-potential-data-breach-details-of-2-crore-users-put-on-sale-on-dark-web/article33056301.ece

[32] Stone Jeff (2016) "*Book Clubs and Paranoid Forums: Tor's Deep Web isn't all bad. Just Crazy*". https://www.inverse.com/article/14104-book-clubs-and-paranoid-forums-tor-s-deep-web-isn-t-all-bad-just-crazy

[33] Mlot Stephanie (2014) "*Facebook releases special link for Tor*". https://in.pcmag.com/social-media/48096/facebook-releases-special-link-for-tor

[34] Dave Lee (2014) "*Facebook sets up 'dark web' link to access network via Tor*", BBC News. https://www.bbc.com/news/technology-29879851

[35] "*BBC News launches 'dark web' Tor mirror*". (2019), BBC News. https://www.bbc.com/news/technology-50150981

[36] Glenn Greenwald (2013) "*The NSA files – Security and liberty. Edward Snowden: the whistleblower behind the NSA surveillance revelations*". https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

[37] J Clement (2019) " Global dark web access technology usage 2019, by country". https://www.statista.com/statistics/1015229/dark-web-access-technology-usage-by-country/#statisticContainer