Xournals

Academic Journal of Forensic Sciences

ISSN: 2581-4273 | Volume 04 | Issue 02 | October-2021

Dark Web – The Hidden Cyberspace

Nitin Pandey[1] and Rahul Pandey[2]

Available online at: www.xournals.com

Received 17th August 2021 | Revised 14th September 2021 | Accepted 26th September 2021

Abstract:

The Dark Web is a small part of the WWW (World Wide Web) whose activities are purposefully covered up and cannot be accessed by normal browsers or search engines and require some particular programs like Tor browser. As the dark web hides the client's identity, it very well may be utilized for legal reasons just as illegal. From sneaking drugs and weapons to other illegal things, from hacking other's data to utilizing those for manufacturing, from duplicating cash to utilizing cryptographic money, the dark web can play various parts in malevolent movements. Then again, the government and other law enforcement agencies utilize the dark web for military applications like online intelligence gathering, sting activity and for other confidential purposes. This paper depicts dark web underlining on how it is accessed, how the tor network works to provide anonymity to its clients, how one can utilize TOR to get to dark web, subtleties on use of dark web for example how unique noxious activities are done utilizing dark web, how the dark web is utilized by terrorist communities to spread terrorism, how the law enforcements are utilizing dark web to reveal some client's real identity and to stop the illegal exercises and the future extent of dark web.

Keywords: *Dark Web, Tor, Tor browser, Surface Web, Deep Web, Silk Road, Terrorism, Cyber Warfare, Data Leaks, Dark Net, Dominos India Server*

Authors:

1. *Cyber Crime Consultant, Police Headquarters Lucknow, Uttar Pradesh, INDIA*
2. *Cyber Security Researcher, B. Tech (CSE), NRCM, Hyderabad, Telangana, INDIA*

Introduction

The Internet can be an unnerving spot. Between phishing, malware and a scope of tricks, there are numerous threats. Yet, there's an even darker corner of the web where not many individuals try to wander: The Dark Web. The Dark Web is a little piece of a much bigger Deep Web–a typical name for an assortment of websites that aren't accessible through ordinary Internet browsers, for example Google chrome. These websites are hidden away from ordinary Internet, or Clearnet. They are based on the frameworks of networks that as of now exist—and there are loads of them. Truth be told, the Deep Web makes up most of the data on the web. It's a territory past the compass of law authorization (henceforth there are no guidelines or security). Although not every person who utilizes the Dark Web participates in illegal exercises, it has a history of being a stage for political protesters and corporate informants.

Most know the Dark Web for its virtual marketplaces loaded with items going from illicit Drugs, stolen credit/debit card details, PayPal accounts, child pornography (pedo films) to prepared malwares and hackers for hire. On the dark web underground markets, a youngster can purchase and sell nearly anything while at the same time remaining absolutely unknown. We're talking about a wide range of illicit drugs (heroin, benzos, Ecstasy, weed, to give some examples), firearms, and Child pornography. Fake cash, taken Visa data, hacked financial data, frauds, taken craftsmanship. To pay for these, one uses bitcoin or different types of cryptographic money.

Teenagers who have fallen prey to sex dealing are publicized here. There are likewise benefits for things like PC hacking and contract killers recruiting. Recordings of creature mercilessness, torture, and murders. It's all stuff that would scare your soul. As anyone might expect, the dark web is mainstream with lawbreakers, pedophiles, and other offensive characters. A raid by the FBI and resulting conclusion of one the most scandalous of these organizations, Silk Road, first made numerous individuals aware of the presence of the Dark Web. The Silk Road was one of the biggest open commercial centers, working similarly like Amazon where outsider vendors could sell their items. In spite of the fact that Silk Road is shut down, and its originator is in jail forever, other illicit businesses still thrive on the dark web.

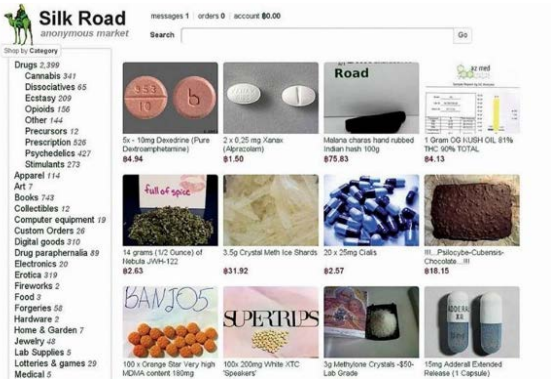

Figure No. 1: Silk Road Homepage

The Silk Road was an online international marketplace for purchasing drugs, collectibles, computer equipment, electronic items, lab supplies etc. It was highly popular for buying/selling of illegal drugs and hosting money laundering activities. It is assumed that the profits made by the silk road between January 2011 and September 2013 was more than 1.2 billion dollars, after which it was destroyed by FBI **(www.wikipedia.org, 2011)**.

Layers of the Internet: Regarding content openness, the whole internet can be separated into three different layers: surface web, deep web, and dark web. The surface web is known as the clear web. Clear Web is the highest layer and incorporates content that is promptly open (indexable) utilizing web search tools. The layer below the surface web is deep web. It's not ordered via web search tools and getting to it frequently requires looking through a data set, or signing into a particular arrangement of substance pages. At long last, at the base layer is the dark web, which is open just with unique programming and frequently utilized for specialty purposes — sometimes criminal, requiring the most elevated level of encryption and obscurity.

Figure No. 2: The categories of Internet

- **The Surface Web:** The surface web is the freely visible piece of the internet that a large portion of us utilize every day, and is obtained through web search tools like Google or Bing. It comprises just 10% of the data that is accessible on the Internet. The Surface Web is essentially the tip of the iceberg.

- **The Deep Web:** This is the piece of the internet which is for the most part hidden away from the general public view. It can't be accessed by means of the standard web crawlers and is reached in other, less broadly known ways. Confidential data like school and clinical records, Personal bank statements and private messages are all stored in the enormous Deep Web. To access this data, you should have the option to get to an overlay network utilizing particular application programs and passwords. This is something to be thankful for in light of the fact that it guards confidential data, and prevents web crawlers from getting and accessing it. The additional security of the Deep Web makes it alluring for the individuals who need their online exercises to stay mysterious. The deep web covers almost 96% to 99% of the whole internet.

- **The Dark Web:** At the point when the majority of the people go on the web, they do so by means of a Personal computer or phone that has an IP (Internet Protocol) address - a unique online identity. Usually, A person's internet action can be monitored by tracking the IP address of their devices.

The 'Dark Web' utilizes complex frameworks that anonymize a client's actual IP address, making it hard to work out which websites a device has visited. The dark web is generally accessed using a special and most popular software program called Tor (The Onion Router).

Around 2.5 million individuals use Tor consistently. Tor itself isn't the 'Dark Web' but a tool that provides accessibility to the dark web as well as the surface web without anybody having the option to recognize the user or track their action.

Method and Methodology

Dark web uses small peer-to-peer networks as well as large networks such as TOR (The Onion Routing Project), I2P (Invisible Internet Project).

TOR (The Onion Router): The Tor browser is specially designed to provide anonymity to its users to enable them enhance their privacy while using the public networks. Users can browse the internet and chat online without having their privacy compromised by the hackers or even to the servers they are communicating with. The ideas supporting Tor in particular, onion directing were created by the United States government during the 1990s. It was initially intended to ensure the interchanges of US knowledge organizations across the Internet. The first code for Tor was delivered under a free and open-source programming permit by the United States Naval Research Laboratory, permitting others and associations to add to the undertaking. Notwithstanding, after it got open to the general population, lawbreakers and radicals started utilizing it for criminal operations. There is no restriction on the dark web, so it's difficult to close down due to the very encryption framework that empowers clients to be covered up. At the point when one site is shut, other fires up surprisingly fast. Since 2006, a non-profit organization called The Tor Project has been liable for keeping up Tor and the Tor Browser. Monetary help comes from companies like Google, associations like Human Rights Watch, and numerous others.

Network traffic analyzers like Wireshark sniff users' packets and know who is talking to whom, at what time has the communication or data exchanges occurred and what kind of data is being exchanged. Encryption of the payloads of the packets does hide the contents, but it does not hide the headers' information which includes the identity of the sender and receiver. Because Tor utilizes the encryption techniques to create tunnels and incorporates indirect server communication, Tor users have the capability to even bypass the websites blocked by the Internet Service Provider.

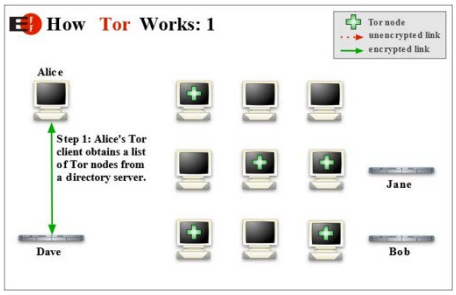

Figure No. 3: How Tor Works 1

Tor disperses an exchange over several places on the Internet, so the destination and source can't be connected by any single point. Rather than taking direct route, information bundles on Tor network take a random pathway through a few relays, so no spectator at any single point can recognize the destination and source of the data packets.

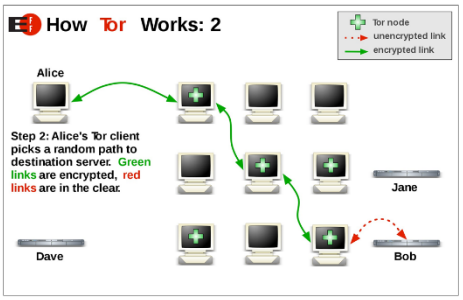

Figure No. 4: How Tor Works 2

To make a private network pathway with Tor, the user's application steadily builds an encrypted circuit connection through the relays on the network. Tor utilizes three relays. The circuit is expanded each jump in turn, so each hand-off just knows the character of the prompt predecessor and relative. The total way taken by an information bundle isn't known to any node. The user utilizes a separate arrangement of encryption keys for each transfer so the encrypted information can be unencrypted by the intended node only. After the circuit is set up, information can be communicated.

Also, to note that, Tor establishes a new connection every ten minutes. It uses the same circuit only for the connection that occurs within 10 minutes. In order to access darknet, other alternative software applications like the freenet and I2P can be used. Though Tor is one of the most popular programs when it comes to providing anonymity, freenet and I2P is also preferable.

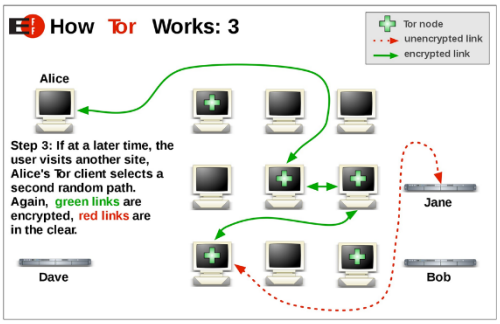

Figure No. 5: How Tor Works 3

1. Payment on the Dark Web

Bitcoin is the cash frequently utilized in exchanges on Dark Web. It is a decentralized advanced money that utilizes mysterious, shared exchanges. People get bitcoins by taking them as a payment, ex-transforming them for traditional cash, or "mining" them. At the point when a bitcoin is utilized in a monetary exchange, the exchange is recorded in a public record, called the square chain. The data recorded in the square chain is the bitcoin addresses of the beneficiary and sender. A location doesn't extraordinarily recognize a specific bitcoin; rather, the location just distinguishes a specific exchange. Clients' locations are related to and stored in a wallet. The wallet contains a person's private key, which is a mysterious number that permits that person to spend bitcoins from the comparing wallet, like a secret key. The address for a transaction and a cryptographic signature are utilized to verify exchanges. The wallet and private key are not recorded in the public record; this is the place where the use of bitcoin has high privacy. Wallets might be facilitated on the web, by application programs for a computer or cell phone, or any other device.

When a bitcoin is utilized in a monetary exchange, the exchange is recorded in a public record, called the block chain. The data recorded in the block chain is the bitcoin addresses of the sender and receiver. An address doesn't extraordinarily recognize a specific bitcoin; rather, the address simply distinguishes a specific exchange. Clients' addresses are related to and stored in a wallet. The wallet contains a person's private key, which is a confidential key that permits that person to spend bitcoins from the wallet, similarly like the passwords

we use. The address for an exchange and a cryptographic digital signature is utilized to verify and confirm exchanges.

The wallet and private key are not recorded in the public record; this is the place where Bitcoin use has uplifted security.

Dominant parts of exchanges on the dark web are done utilizing Bitcoin, which is one of the first and best digital forms of money and it is utilized basically for its utilization of block chain technology with no central man like a bank. So, individuals can get a wallet and nobody will know what their identity is.

2. Internet Governance and Legal Implications

Looking at the growth of users browsing the darknet for illegal activities, the Defense Advanced Research Projects Agency (DARPA) dispatched a program in 2014, called Memex. Their point is to develop a search index to help the law enforcement agencies identify human trafficking tasks on the darkweb. As indicated by them, Business web search tools like Google or Yahoo look through websites' dependent on their prominence and files around 5 % of the whole Internet, however Memex aims to give a superior output by moving through all the websites that are overlooked by business web search tools and on the profound web just as dark web **(www.darpa.mil, 2014)**

Memex will incorporate three specialized zones:

a) **Domain Specific Indexing**, which would incorporate a web crawling framework that could incorporate such highlights as natural language processing, picture analysis, interactive media extraction etc. It likewise ought to be impervious to counter-slithering measures, bot discovery and other barriers to the extraction of data.

b) Domain Specific Search, which would incorporate a Domain specific interface that can be arranged for an individual, explicit kinds of substance, location and other different factors. DARPA would likewise expect engineers working in these initial two areas to create and query language equipped for directing the searches.

c) Applications, which include creating applications to help specialized regions 1 and 2, beginning with applications that help endeavors to counter human trafficking **(www.defensesystems.com, 2014).**

Analysts are proceeding to figure out how arising innovations can be customized to what law enforcement agencies need and for how the dark web works. Connecting clients on the dark web is the thing that law authorization as of now attempts to do. The issue is that the measure of information that they need to manually rearrange through is excessively large and unstructured for them to discover associations rapidly. Consequently, just a low level of cases can be pursued.

To computerize the same, Lincoln Laboratory is preparing Artificial Intelligence algorithms to process the comparability between clients on various forums. The algorithm is first given data from clients on a given Forum 1 and makes an initiation model for every client. At that point, information from clients on Forum 2 are run against all client models from Forum 1. To discover matches for profile data, the calculation searches for direct signs, for example, changes in username spelling like "SilkRoad" on Forum 1 to "Silk Street" on Forum 2.

Another feature of this algorithm is looking for content similarity. The framework searches for similarities in a client's network, which is the circle of individuals that the client collaborates with, and the points that the client's network examines. The profile, substance, and network highlights are then combined to give a solitary output: a likelihood score those two personas from two gatherings address a similar real-life individual. The scientists have been trying these persona-connecting calculations both with open-source Twitter and Instagram information and hand-named ground truth information from dark-web gatherings **(news.mit.edu, 2019).**

Cyber criminals are keen on data sets, monetary data, private messages and trade secrets. These Cyber Criminals compromise this information through phishing assaults and other malware. This information falling under the control of cyber criminals will put your business in danger and the entirety of this is planned, arranged and executed in the Dark Web. To battle this, CYFIRMA, A product organization situated in Singapore has fostered a Cyber Intelligence model called 'DeCYFIR'. In the

Model, a huge number of automated agents/bots are sent to monitor the dark web and give all day, every day observation **(www.cyfirma.com, 2020)**.

A Cyber security monitoring model is being developed by the government of India, which will be providing help to the law enforcement in tracking cyber criminals utilizing the dark web to buy and sell different illegal products. CDAC (Centre for Development of Advanced Computing) is working with the CSIR on building up a darknet/network telescope-based digital monitoring and interference framework **(www.financialexpress.com, 2018).**

Results and Discussion

Clients of TOR communicate with one another using email services, real-time chat rooms like Onion Chat, the hub etc. Bit message and Ricochet are other messaging alternatives accessible on TOR. The hidden Wiki is a website that contains a directory of covered up .onion sites arranged as websites for drugs, whistleblowing sites such as WikiLeaks, weapons, crypto currency sites, child abusive content, social networking sites etc. A significant weakness of Tor is its slow speed since all TOR traffic is sent through numerous transfers and there can be delays in any of the middle hubs. Speed is diminished at the point when more clients are at the same time utilizing TOR networks.

Another option of utilizing TOR is TOR2WEB. This product allows users to access content on the dark web from a simple browser without being connected with the TOR network. Here the user does not need to install and run the tor browser in order to access .onion sites. Yet, it doesn't give the same level of anonymity to users which is given by TOR.

Every coin has two sides and so does the dark web. Below are some of the legal and illegal use of the dark web.

Legal Use of Dark Web

- Journalists: Journalists utilize the dark web to speak with informants to get delicate information and to namelessly write on politically touchy issues.
- Law enforcements: while the dark web is accepted to be intensely utilized for unlawful work, law authorization specialists utilize dark web to recognize the illicit works furthermore, stop them.

For law authorization, TOR is commonly used. There are two fundamental activities for law enforcements use:

a) Online Surveillance: TOR permits officials to surf .onion sites and services which are problematic providing full anonymity and not leaving any traces.

b) Sting Operations: TOR's anonymity permits law officers to take part in secret tasks.

- Residents of some countries like China (which forces a few limitations on the utilization of Internet and utilization of Google, Facebook and other well-known destinations) utilize dark web to get to them secretly.
- The greatest benefit of utilizing the Dark Web is its Anonymity. Not everyone accessing the dark web has bad intentions. A few users may worry about their online privacy and security. They need their Internet movement to be kept hidden.

Illegal Use of Dark Web

The Dark Web is the center of criminal assaults as it gives Anonymity and goes about as an entryway to the world of crime.

Drug trafficking: The dark web is an unlawful dispensary of illegal and dangerous substances (drugs) that are sold in return of cryptocurrencies. The dark web's biggest darknet market which was begun by a Canadian, was shut down by the U.S Police. Silk Road was additionally one of the well-known commercial centers for unlawful medications and unlicensed drugs. Presently alpha bay, Wall Street market, dream market etc. are some of the most popular marketplaces for buying and selling drugs.

Human trafficking: A dark place namely “Black Death” is an onion site on the dark web where most of the human trafficking happens. Chloe Ayling, the British model is one of the casualties of Dark web's human trafficking practice. As indicated by a 2017 report, the majority of the overcomers of human trafficking were enlisted for sex trafficking and work trafficking **(www.wikipedia.org, 2021)**.

Child Pornography: Child pornography produces the most traffic to the sites on TOR. It is a demonstration that misuses the children for sexual incitement and abuse of kids during sexual demonstrations. It additionally contains naked pictures of children's being abused. A site known as Lolita City which has now been brought down by the Anonymous group of hackers as it contained over 100GB of photographs and recordings of youngster erotic entertainment and has around 15,000 individuals **(BBC News, 2011).**

Playpen was brought somewhere near the FBI in 2015 which may have been the biggest child erotic entertainment webpage on the whole dark web with more than 200,000 individuals **(www.wikipedia.org)**

Frauds: Carding frauds are selling stolen credit/debit card information. It is the most widely recognized sort of wrongdoing that occurs on the Dark Web. There are a huge number of websites that offer stolen credit/debit card information in the darknet including PayPal accounts.

Not only debit and credit cards but pharmaceutical frauds are on the rise. In this pandemic, several onion sites on the Dark Web showed Covid-19 antibodies available to be purchased, for example, clusters of 1,000 shots of Russia's Sputnik V for $4,000 worth of bitcoin or 800 shots of the Pfizer Inc. what's more, BioNTech SE immunization for $20,000 in bitcoin. Vaccination certificates are additionally possible to buy on the dark web **(www.wsj.com, 2021).**

Arms Trafficking: Dark web has now become a popular platform for arms trading. According to the research of a team from Michigan State University, around 64% of the products traded on the dark web were handguns, 17 per cent semi-automatic long guns and fully automatic long guns were around 4 per cent.

Contract killer: Dark web is additionally a stage for recruiting hired gunmen. It is a stage where a professional killer can be hired.

Torture: Red Rooms are sites where clients pay in thousands to see streaming killings, assaults, child pornography and different sorts of torture. In any case, there is still no proof that the red rooms exist. On the off chance that they do exist, they can't be accessible through TOR as TOR is too slow for streaming live videos.

Daisy's destruction is a snuff film produced by Peter Scully and his crew members in the company, "No Limits Fun". Daisy's destruction is a video found on the dark web showing the brutal abuse, torture, rape and murder of 3 young girls. Daisy was confirmed to be only 19 months old at the time, while Liza and Cindy were both 11 and 12 years old. Fortunately, Peter Scully was found and put in life imprisonment.

Revenge porn: Revenge porn is sharing of sexual images and recordings of people without their permission. 'Pink Meth' is one of the popular sites which operates on the dark web where clients can upload nude images of their ex-girlfriends which will lead to harassment of the individual in the image. The website is presently shut down, however there are claims that there's another website that has started up since its end.

Cyber Warfare: ISIS and other terrorist groups use the darknet to communicate with likeminded people and hire them. These people plan attacks and also raise funds for their projects. These terrorists communicate with other members using encrypted messaging applications such as Telegram **(Weimann, 2015)**.

Data Leaks: Your Personal information has been taken; however, you will not find out about it until the organization you've trusted with your data tells you that your contact details, home address, phone number, Debit/Credit card details or some other piece of confidential data has been compromised in a data breach.

With your taken data, hackers can do everything from making buys and opening up credit accounts in your name to petitioning for your income tax refunds, all acting like "you." What's more regrettable, billions of these hacked login details and credit/debit card information are accessible on the dark web at a dirt-cheap price.

On April 16, 2021, Hackers declared that they compromised the Domino's India servers and downloaded 13 TB of information consisting of employees and customer's data. The hackers guaranteed that they got more than 1,000,000 credit card details used to put orders on the application. This information has gotten public as hackers have

made a search engine on Dark web on May 21, 2021. On the off chance that you are a regular Dominos purchaser, you are well on the way to track down your own information there. The data that has been spilled incorporates the name, email, telephone number and surprisingly the GPS area of customers **(www.resonantnews.com, 2021)**.

Conclusion

There are a number of future headings in which associations and clients can work to shield themselves from such sort of crimes which occur over the Dark Web. For associations, there is a need to understand the dangers which are presented by the Dark Web and those presented by remote access Trojans and malwares especially. Associations must use their capacity to utilize the Dark Web for intelligence gathering by monitoring darknet marketplaces. Dark web has consistently been an interesting topic for analysts. Despite the fact that it is strengthening its roots hiddenly, Majority of internet users have no idea about the dark web. While the dark web is only a small part of the deep web, the activities taking place there is something to worry about. As the dark web is turning into a favorable place for crimes, law enforcement agencies are attempting to deanonymize websites and uncover the identities behind those websites. Considering the future of the dark web it can be said that the dark web will turn out to be darker. Number of dark web clients is expanding step by step. Terrorist groups like Al-Qaeda and other jihadists in Libya and Syria are spreading their vision through the dark web. They are utilizing it for recruiting individuals across the world and planning attacks. Selling and purchasing stolen credit card details, cloned credit cards, medical details, passport details etc. are emerging as new crimes in the dark web which is a major threat to the society. The activities of whistleblowers are increasing day by day using the dark web. After the shutdown of three major darknet markets by law enforcement, the hosts of darknet markets are strengthening the security of their websites to make it difficult for law enforcement to track the sites. It can be concluded that the people can use dark web for privacy purposes and stay anonymous on the internet as the use of dark web is not illegal until the user does not involve in any activity that is illegal under the law. The advantages and disadvantages of the Dark Web depend upon what the user's intentions are.

References:

"Abduction of Chloe Ayling." *Wikipedia*, Accessed Date 11th June 2021, Accessed from en.wikipedia.org/wiki/Abduction_of_Chloe_Ayling.

"Artificial Intelligence Shines Light on the Dark Web." *MIT News | Massachusetts Institute of Technology*, 13 May 2019, Accessed Date 11th June 2021, Accessed from news.mit.edu/2019/lincoln-laboratory-artificial-intelligence-helping-investigators-fight-dark-web-crime-0513.

BBC News. "Hackers Take down Child Pornography Sites." *BBC News*, 24 Oct. 2011, Accessed Date 11th June 2021, Accessed from www.bbc.com/news/technology-15428203.

"Deep and Dark Web Monitoring." *CYFIRMA*, 1 June 2020, Accessed Date 11th June 2021, Accessed from www.cyfirma.com/deep-and-dark-web-monitoring.

"Memex (Archived)." *Defense Advanced Research Projects Agency*, 2014, Accessed Date 11th June 2021, Accessed from www.darpa.mil/program/memex.

"Memex: The next Generation of Deep-Web Search? -." *Defense Systems*, 11 Feb. 2014, Accessed Date 11th June 2021, Accessed from defensesystems.com/articles/2014/02/11/darpa-memex-next-gen-search.aspx.

Online, F. "Govt Working on Developing System to Track, Analyse Data from Dark Web." *The Financial Express*, 19 Feb. 2018, Accessed Date 11th June 2021, Accessed from www.financialexpress.com/industry/technology/govt-working-on-developing-system-to-track-analyse-data-from-dark-web/1072111.

Orru, Mauro. "Dubious Covid-19 Shots, Fake Vaccination Certificates Proliferate on Dark Web." *WSJ*, 5 May 2021, Accessed Date 11th June 2021, Accessed from www.wsj.com/articles/dubious-covid-19-shots-fake-vaccination-certificates-proliferate-on-dark-web-11620207001.

"Playpen" (Website). *Wikipedia*, Accessed Date 11th June 2021, Accessed from en.wikipedia.org/wiki/Playpen_(website).

Rnewsauthor. "Why Should Domino's Data Leak Concern Me?– EXCLUSIVE." *Resonant News*, Accessed Date 11th June 2021, Accessed from resonantnews.com/2021/06/14/why-should-dominos-data-leak-concern-me.

Silk Road (Marketplace). *Wikipedia*, 11 June 2011, Accessed Date 11th June 2021, Accessed from en.wikipedia.org/wiki/Silk_Road_(marketplace).

Weimann, Gabriel. "Going Dark: Terrorism on the Dark Web." *Studies in Conflict & Terrorism*, vol. 39, no. 3, 2015, pp. 195–206. *Crossref*, doi:10.1080/1057610x.2015.1119546.